

53. 相互に暗号データの転送を実行する第1の装置と第2の装置とからなるデータ処理システムにおけるデータ処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、

上記第1の装置から上記第2の装置に転送されるコマンド識別子を予め定められた設定シーケンスにしたがって受領し、該受領コマンド識別子に対応するコマンドをレジスタから取り出して実行させるコマンド処理制御ステップを有し、

上記コマンド処理制御ステップにおいて、上記第1の装置から転送されるコマンド識別子が上記設定シーケンスと異なるコマンド識別子である場合には、該コマンド識別子に対応するコマンドの処理を中止するステップを含むことを特徴とするプログラム提供媒体。

BEST AVAILABLE COPY

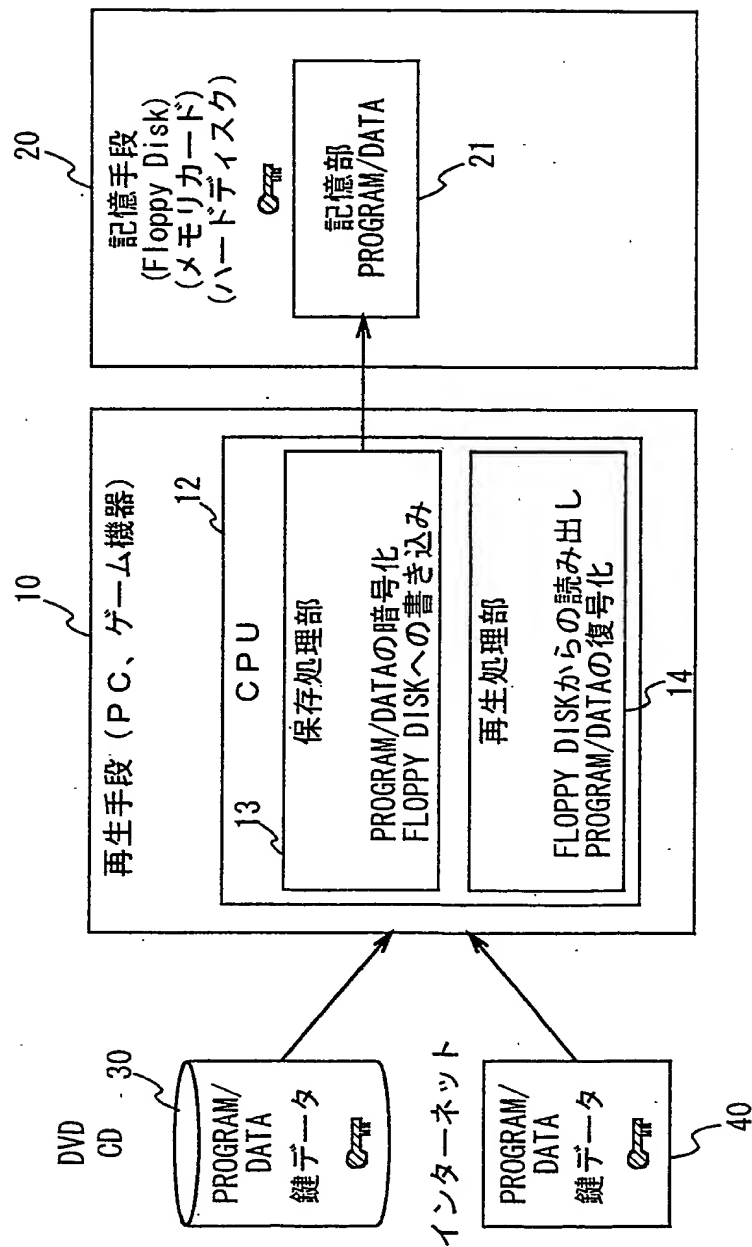


図 1

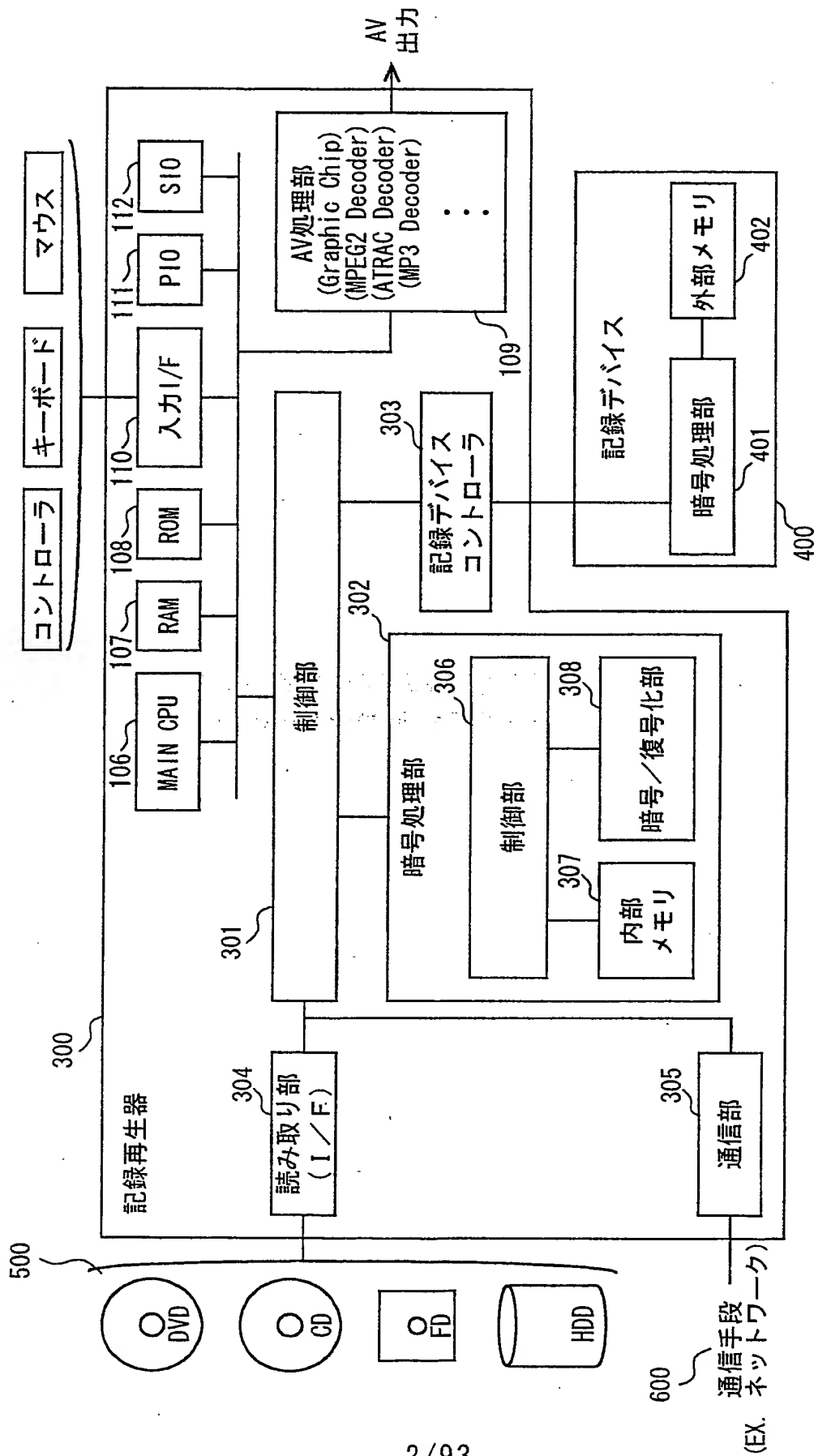


図 2

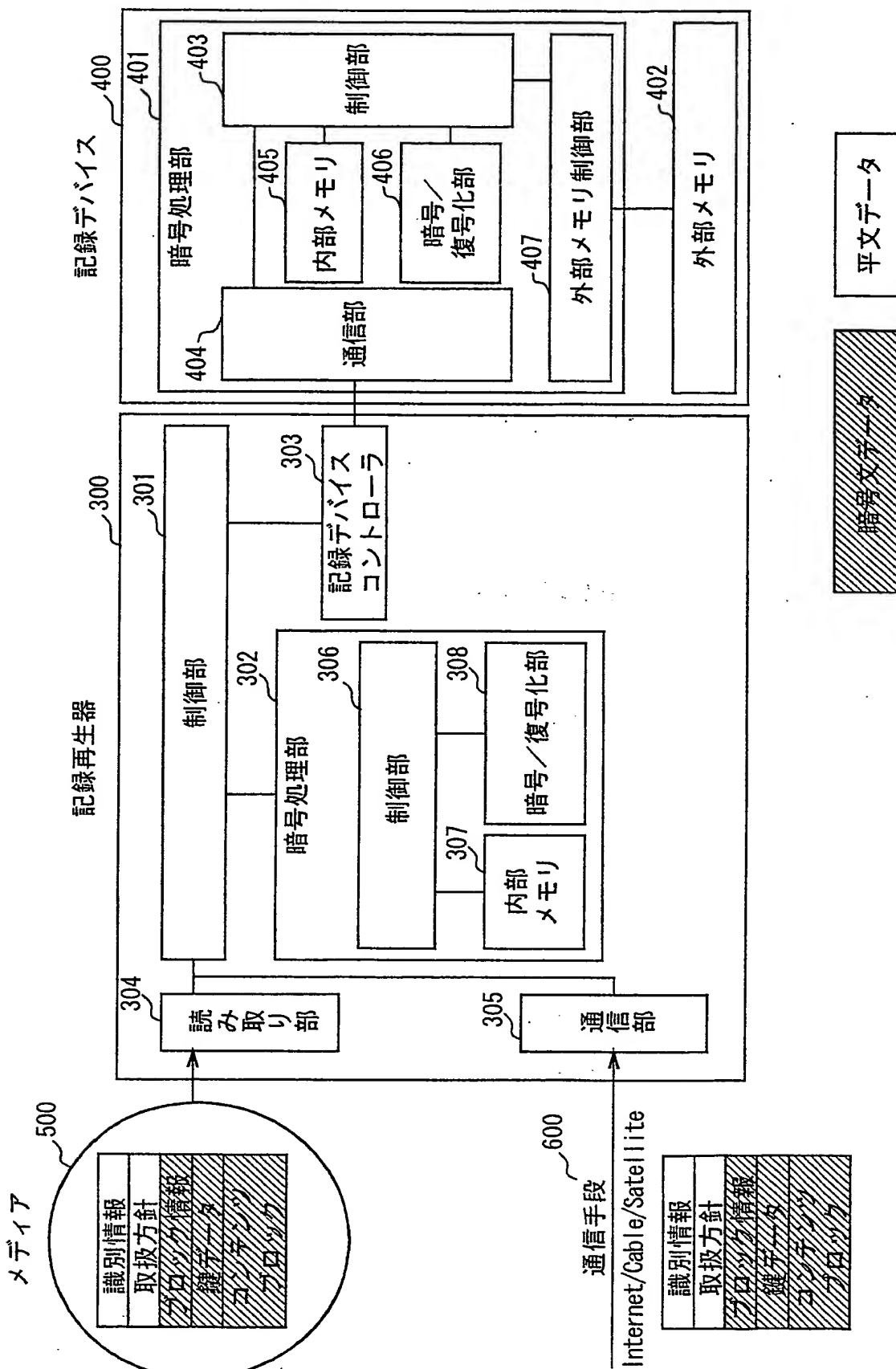
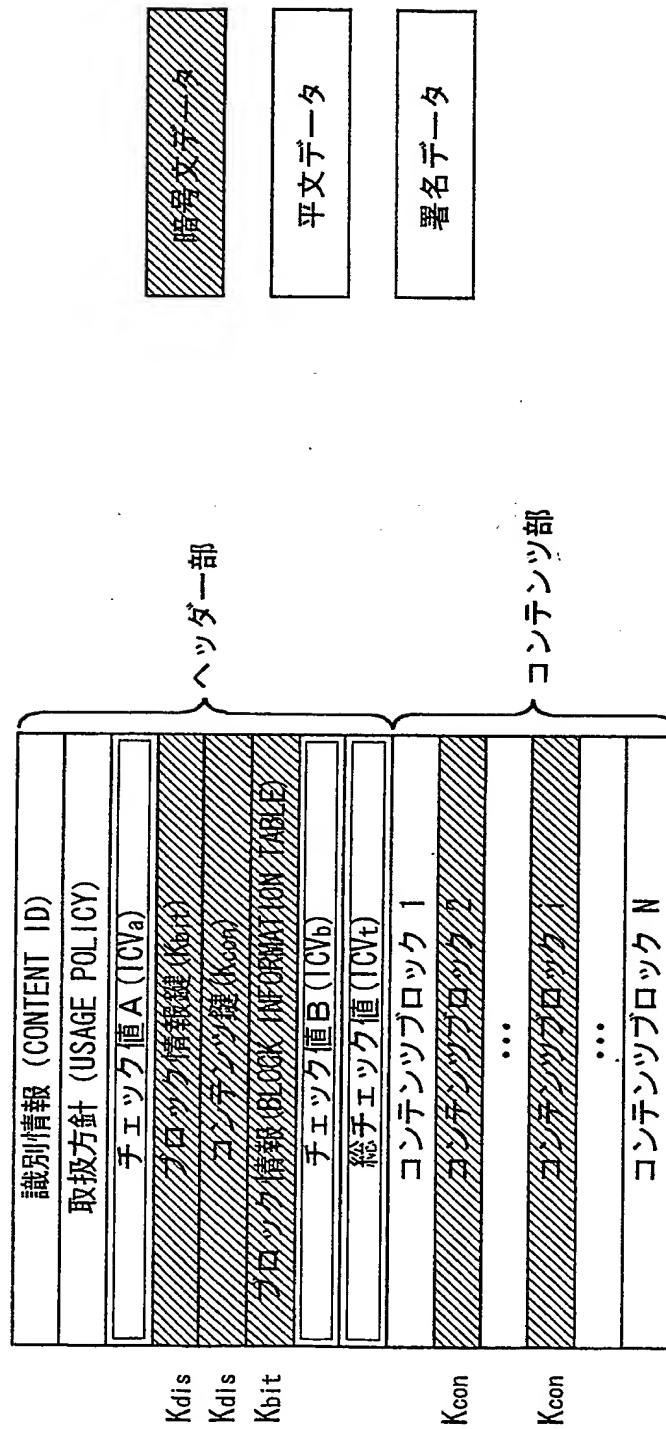


図3



メディア上及び通信路上のデータフォーマット

図 4

ヘッダーサイズ (Header Length)
コンテンツサイズ (Content Length)
フォーマットバージョン (Format Version)
フォーマットタイプ (Format Type)
コンテンツタイプ (Content Type)
起動優先順位情報 (Operation Priority)
利用制限情報 (Localization Field)
複製制限情報 (Copy Permission)
移動制限情報 (Move Permission)
暗号アルゴリズム (Encryption Algorithm)
暗号化モード (Encryption Mode)
検証方法 (Integrity Check Method)

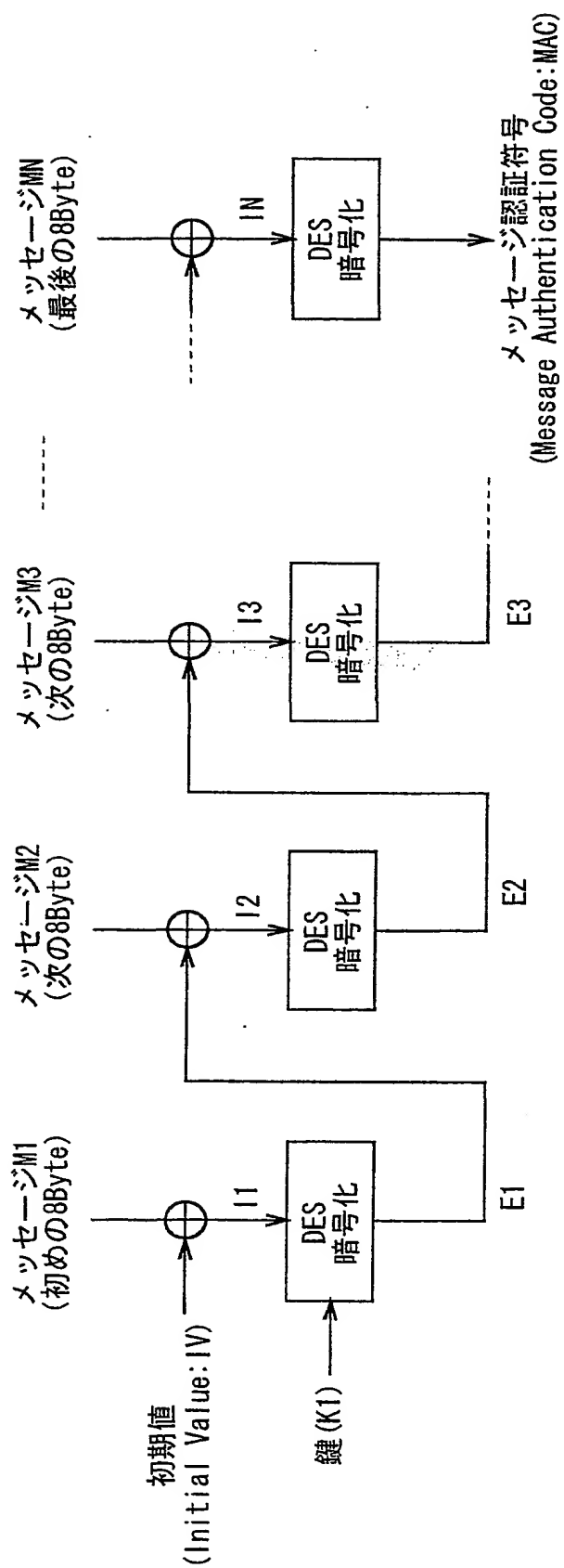
取扱方針

図 5

Kbit ブ ロ ッ ク 1	コンテンツブロック数 (Block Number)	
	ブ	ブロックサイズ (Block Length)
	ロ	暗号化フラグ (Encryption Flag)
	ッ	検証対象フラグ (ICV Flag)
	ク	コンテンツチェック値 (ICV1)
.		
.		
.		
.		
ブ ロ ッ ク N	ブ	ブロックサイズ (Block Length)
	ロ	暗号化フラグ (Encryption Flag)
	ッ	検証対象フラグ (ICV Flag)
	ク	コンテンツチェック値 (ICVN)

ブロック情報

図 6



⊕: 排他的論理和処理 (8バイト単位)

図 7

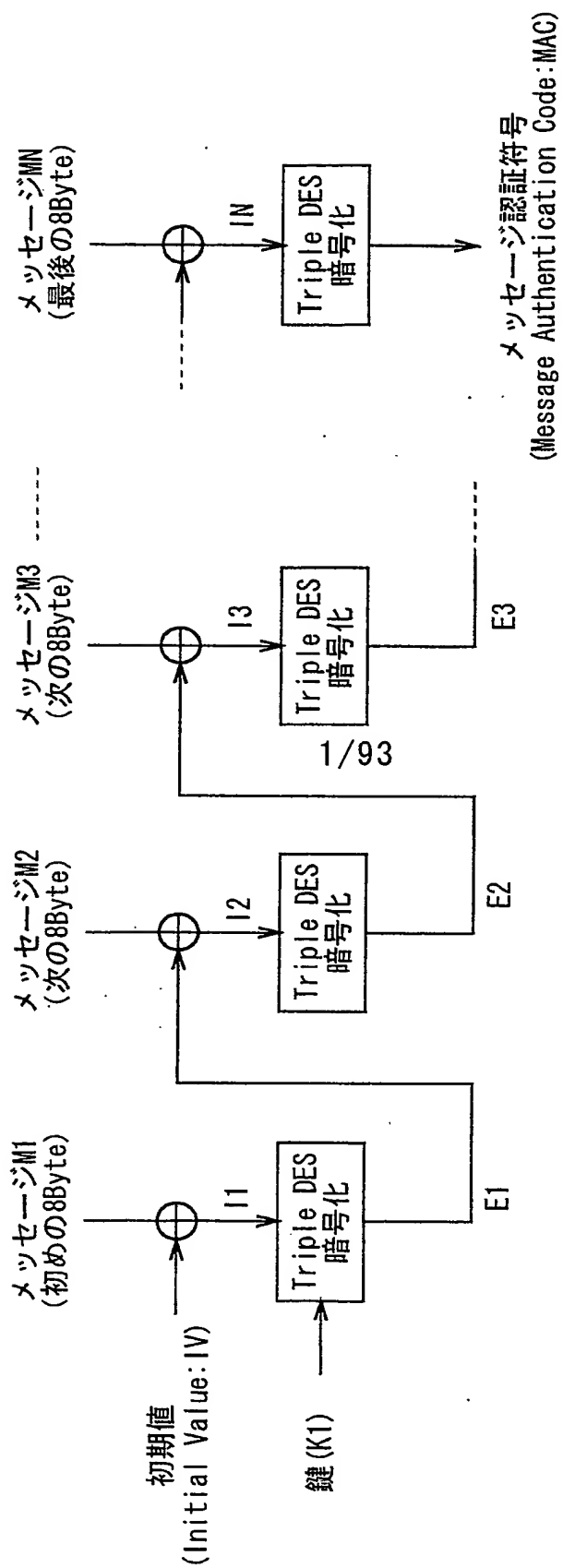


図 8

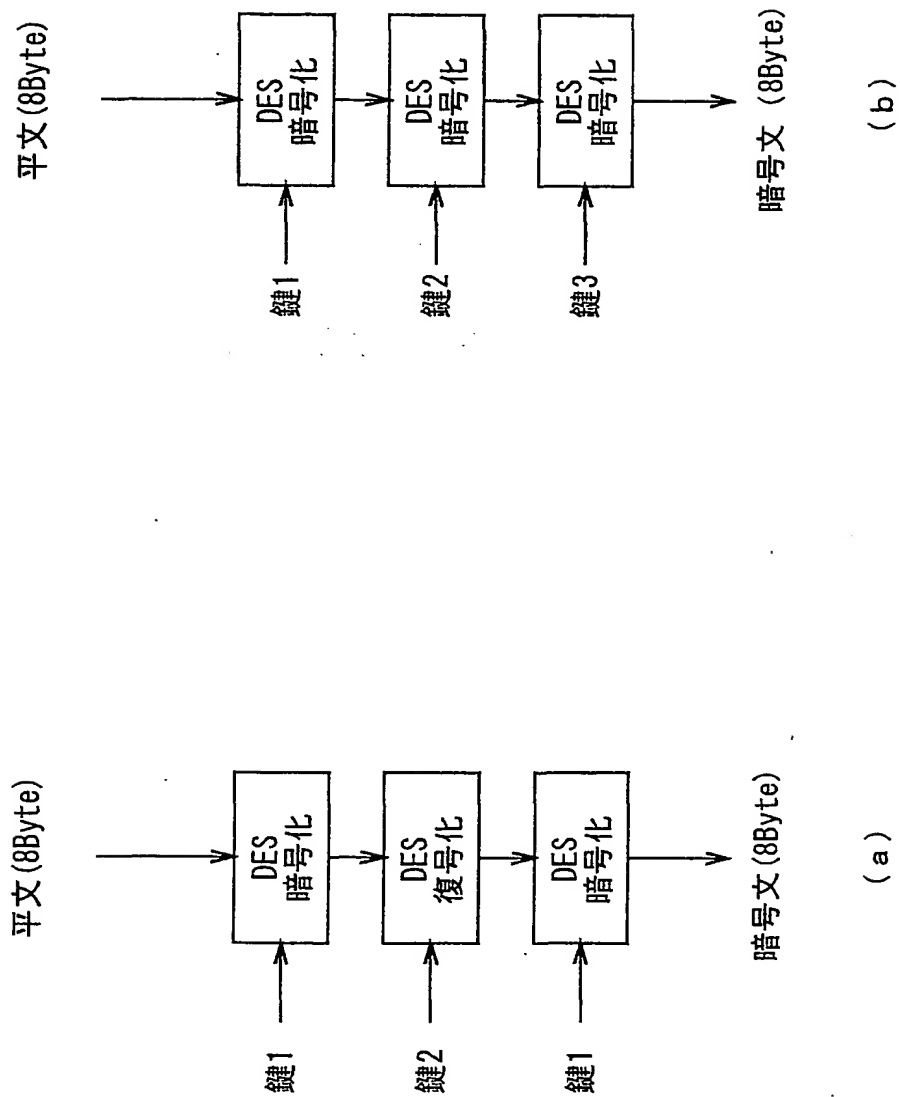


図 9

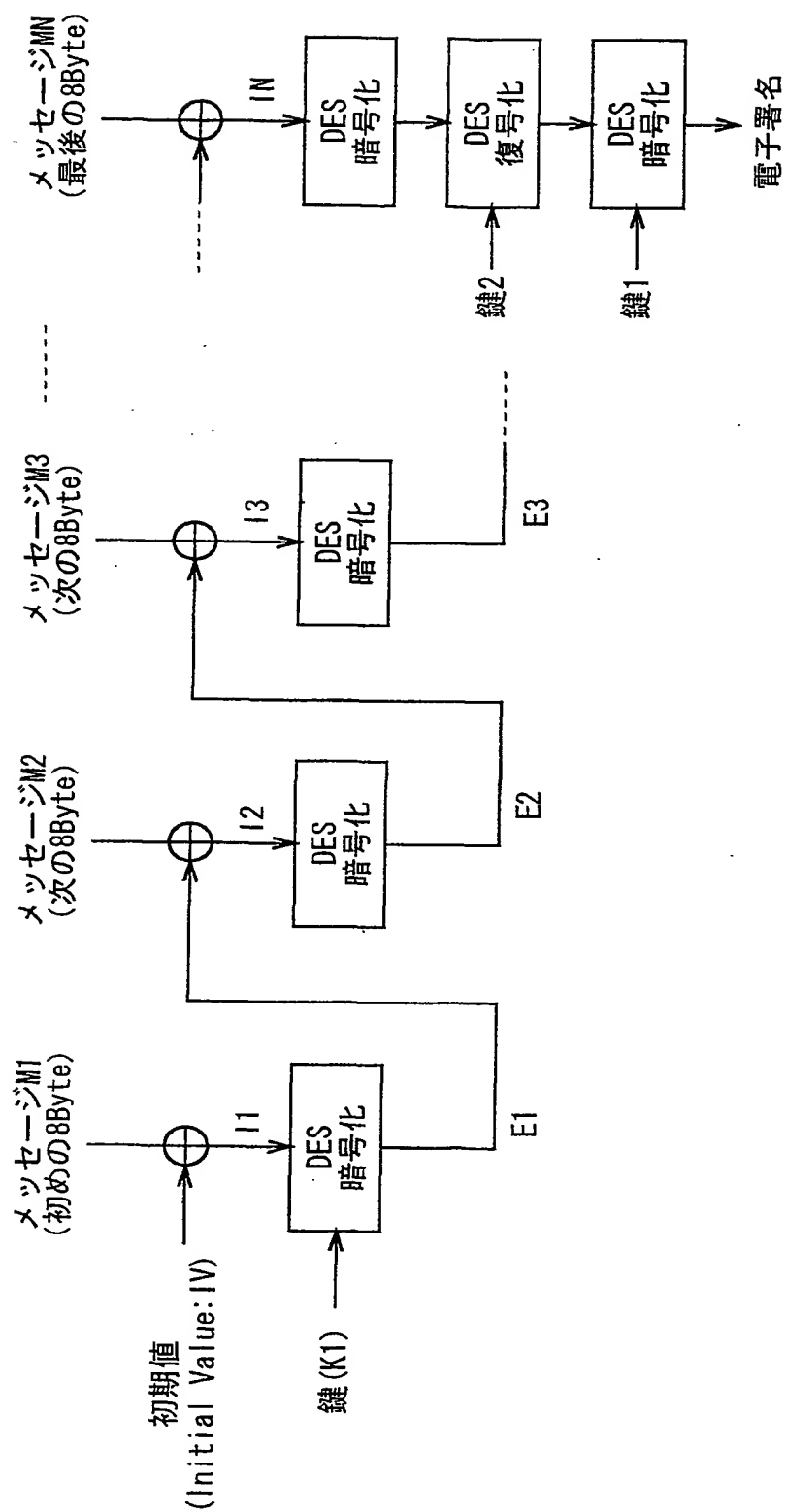
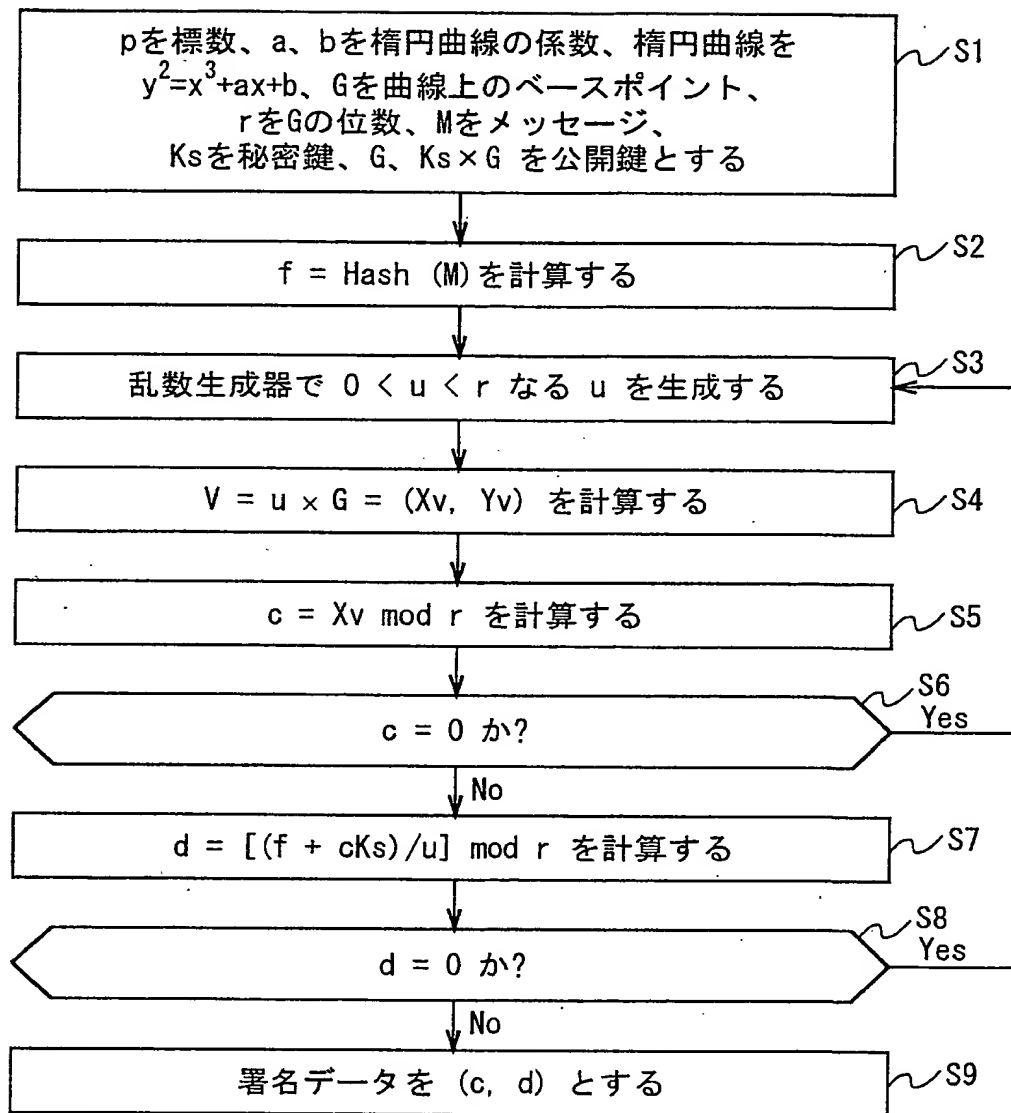


図 10

署名生成署名生成 (IEEE P1363/D3)

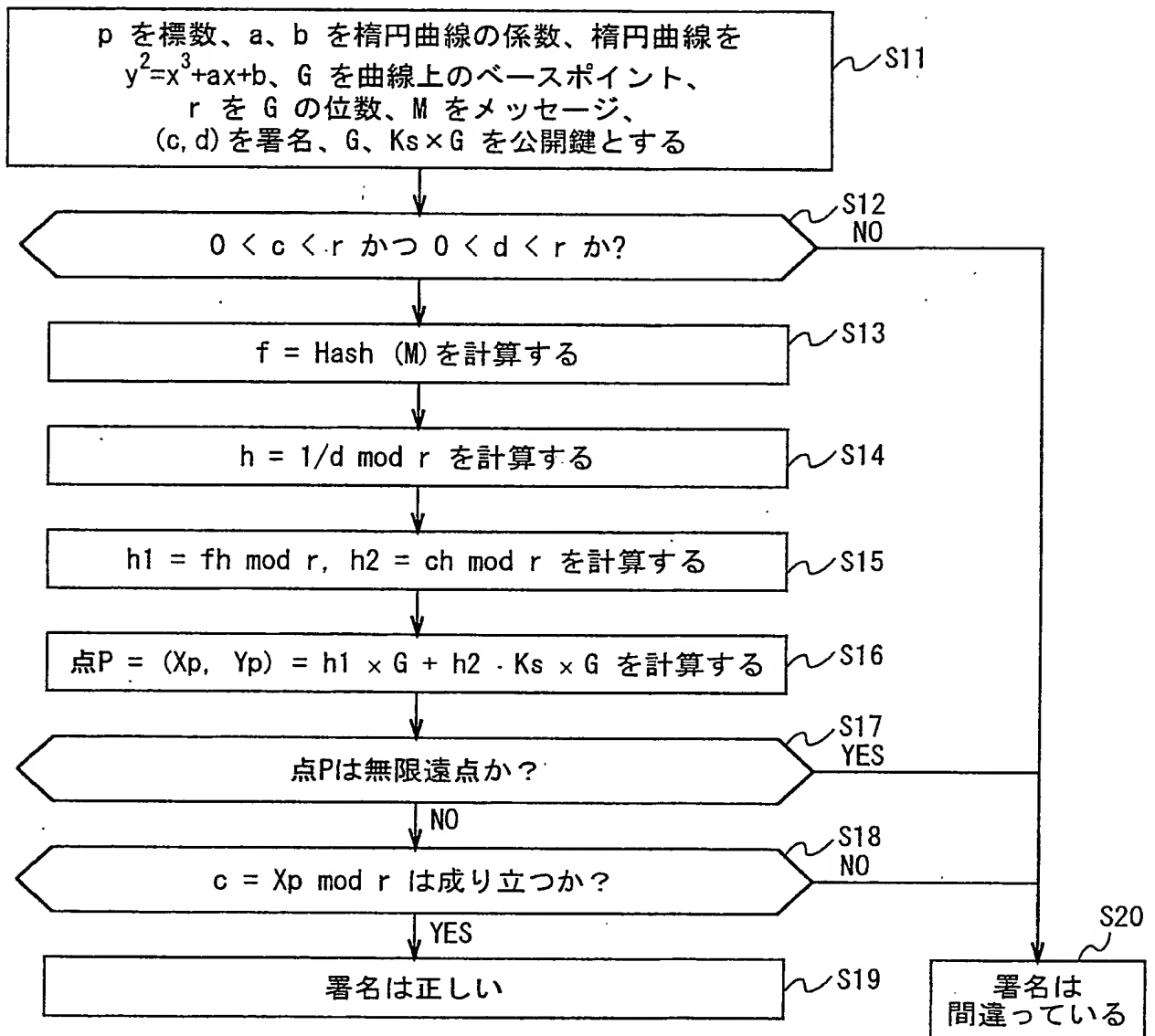
署名検証署名検証 (IEEE P1363/D3)

図 1 2

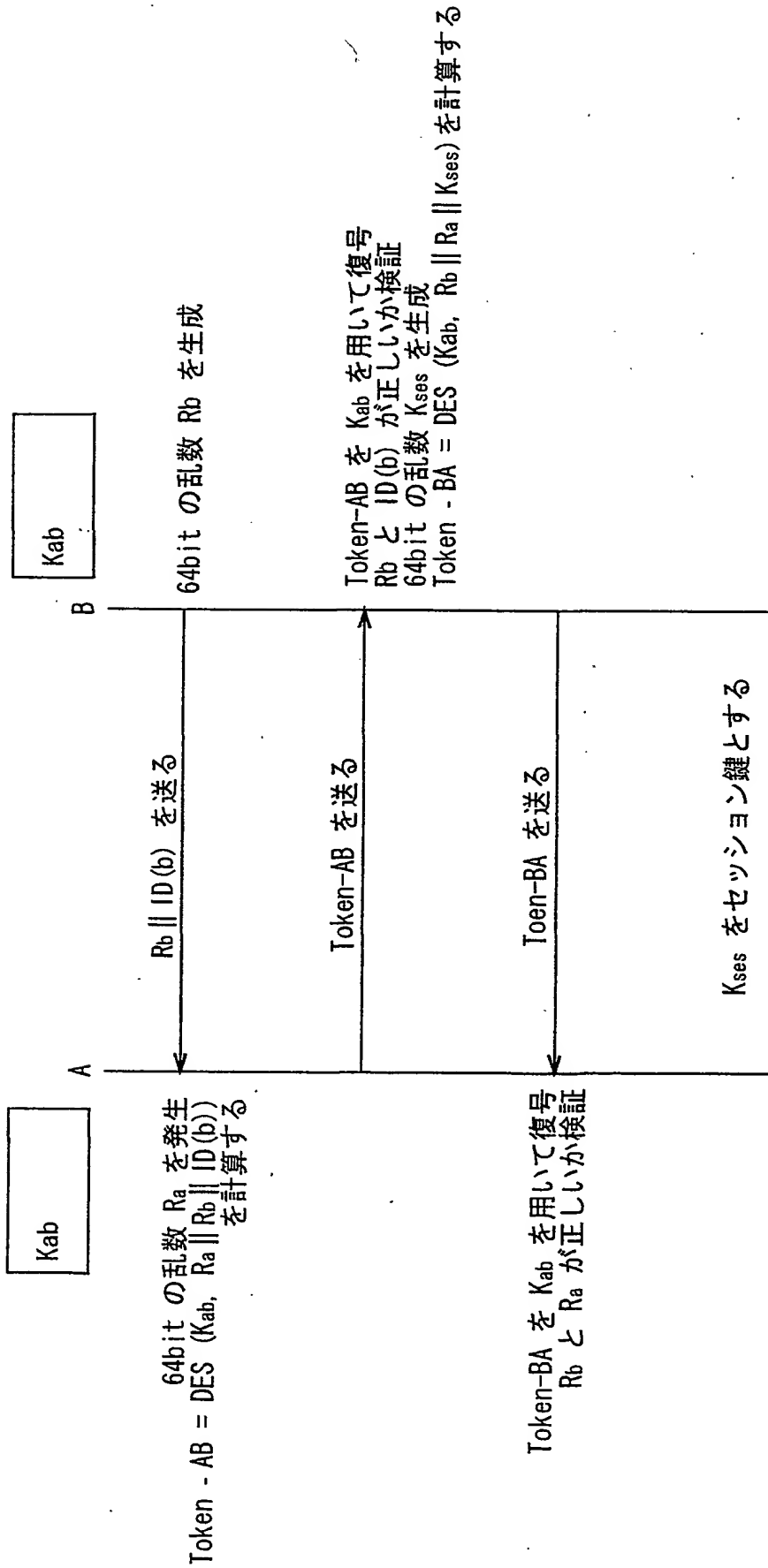
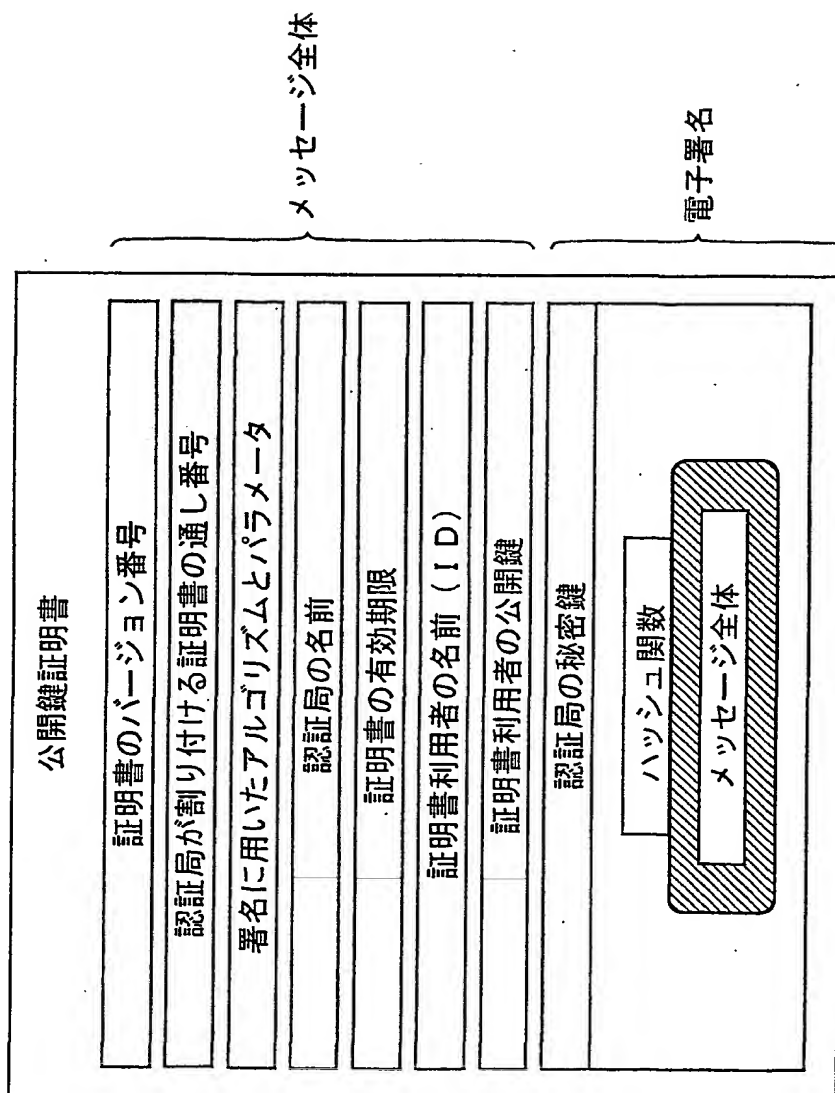


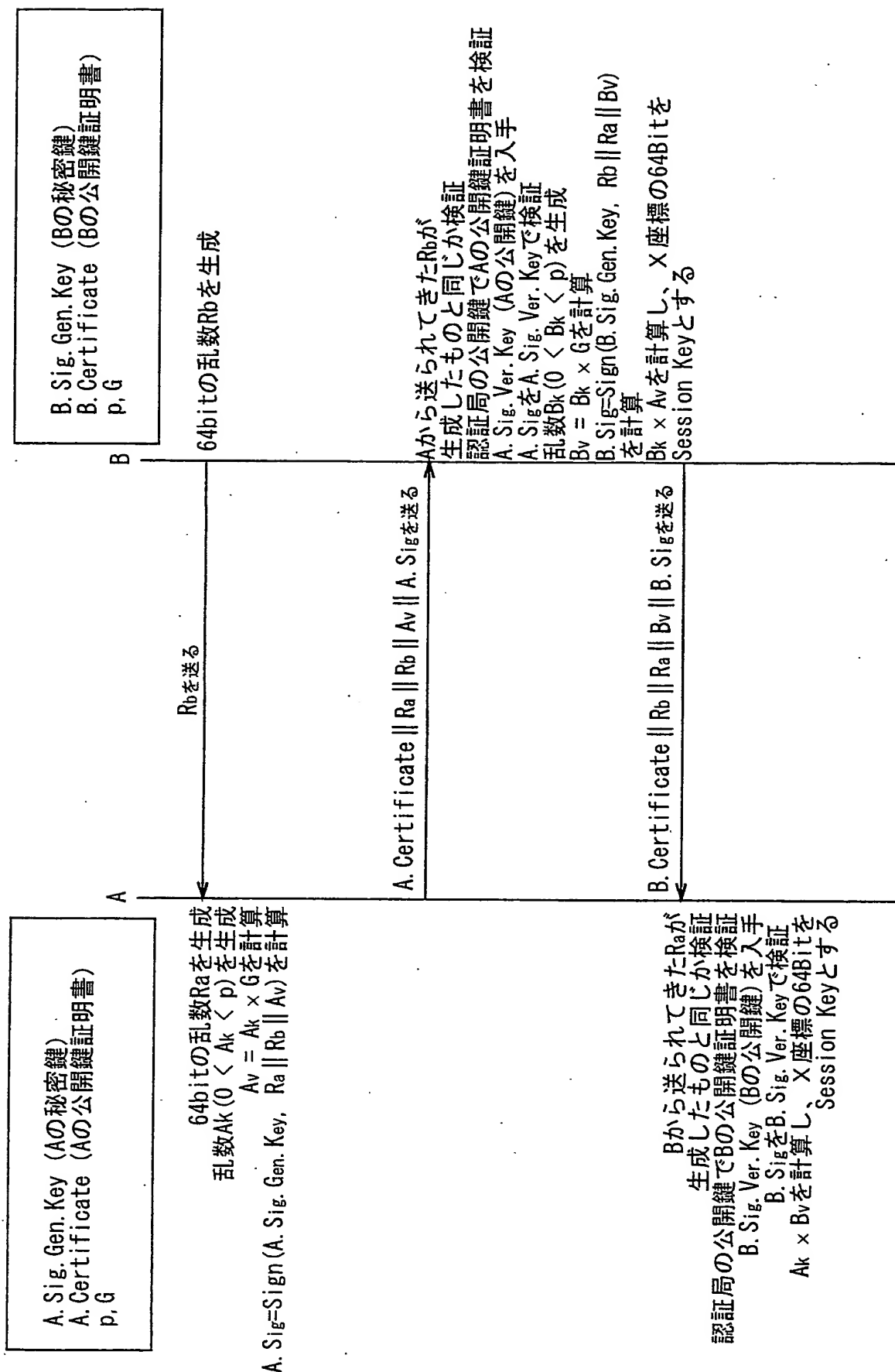
図 1-3

ISO/IEC 9798-2 対称鍵暗号鍵技術を用いた相互認証および鍵共有方式

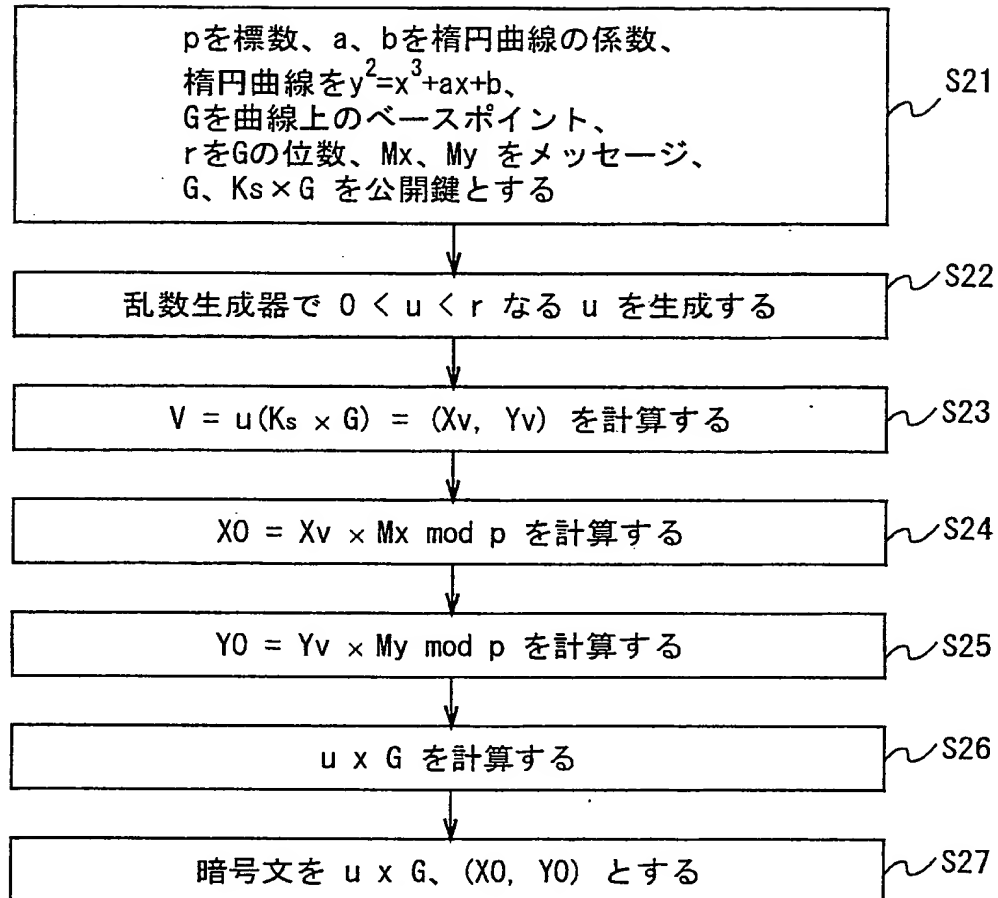


公開鍵証明書

図 14



ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

暗号化

楕円曲線暗号を用いた暗号化 (Menezens-Vanstone)

図 1 6

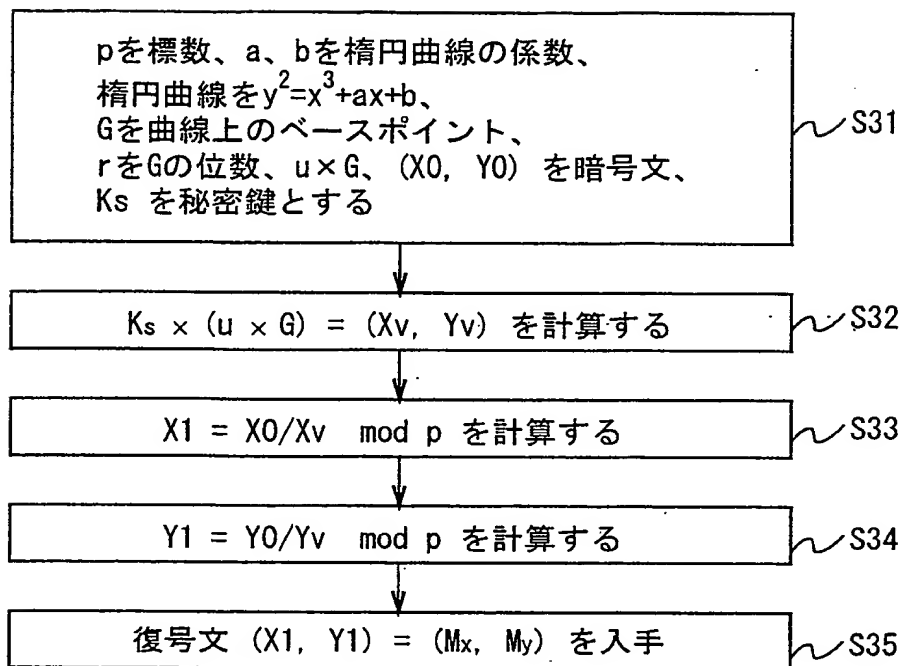
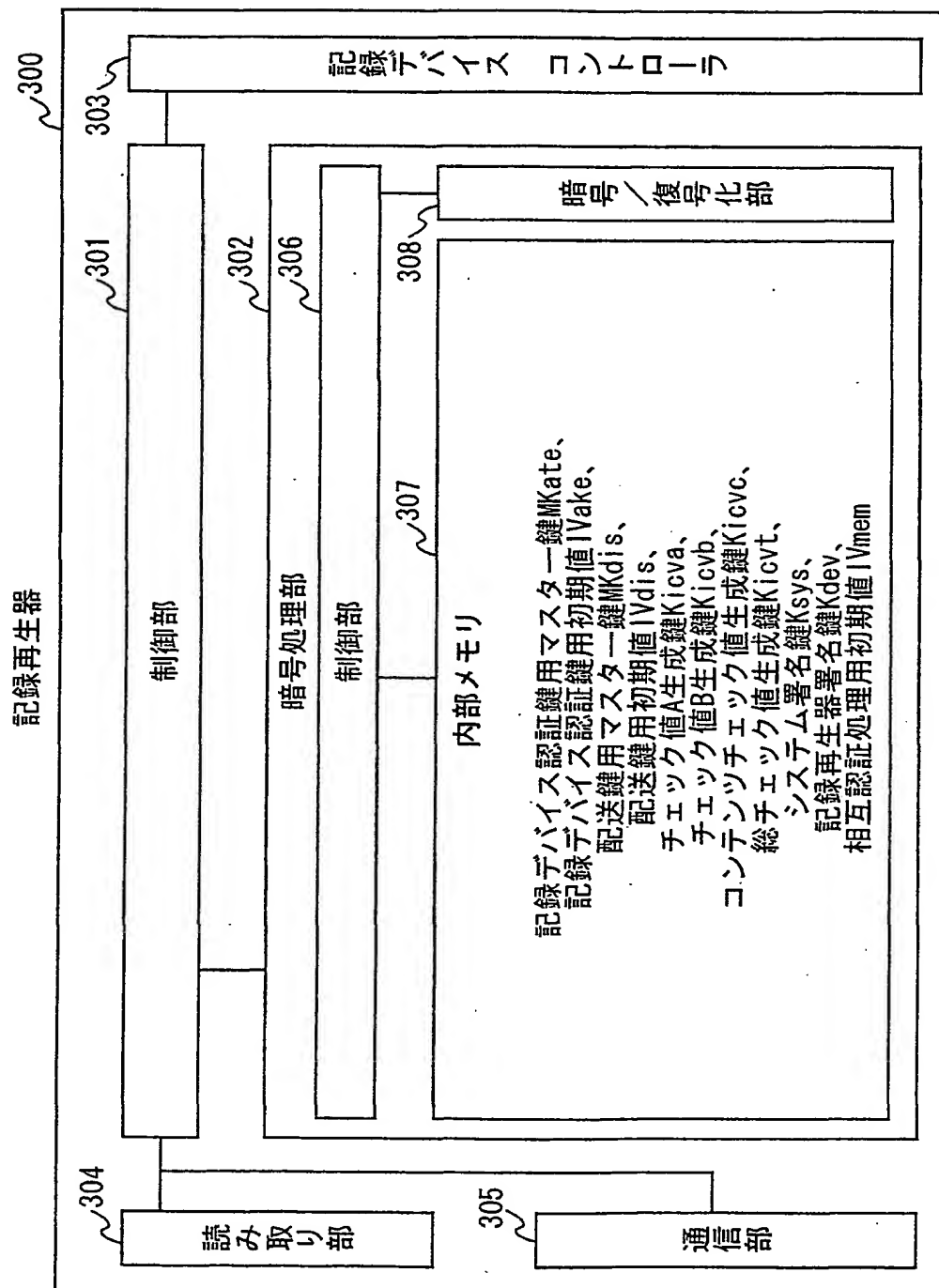
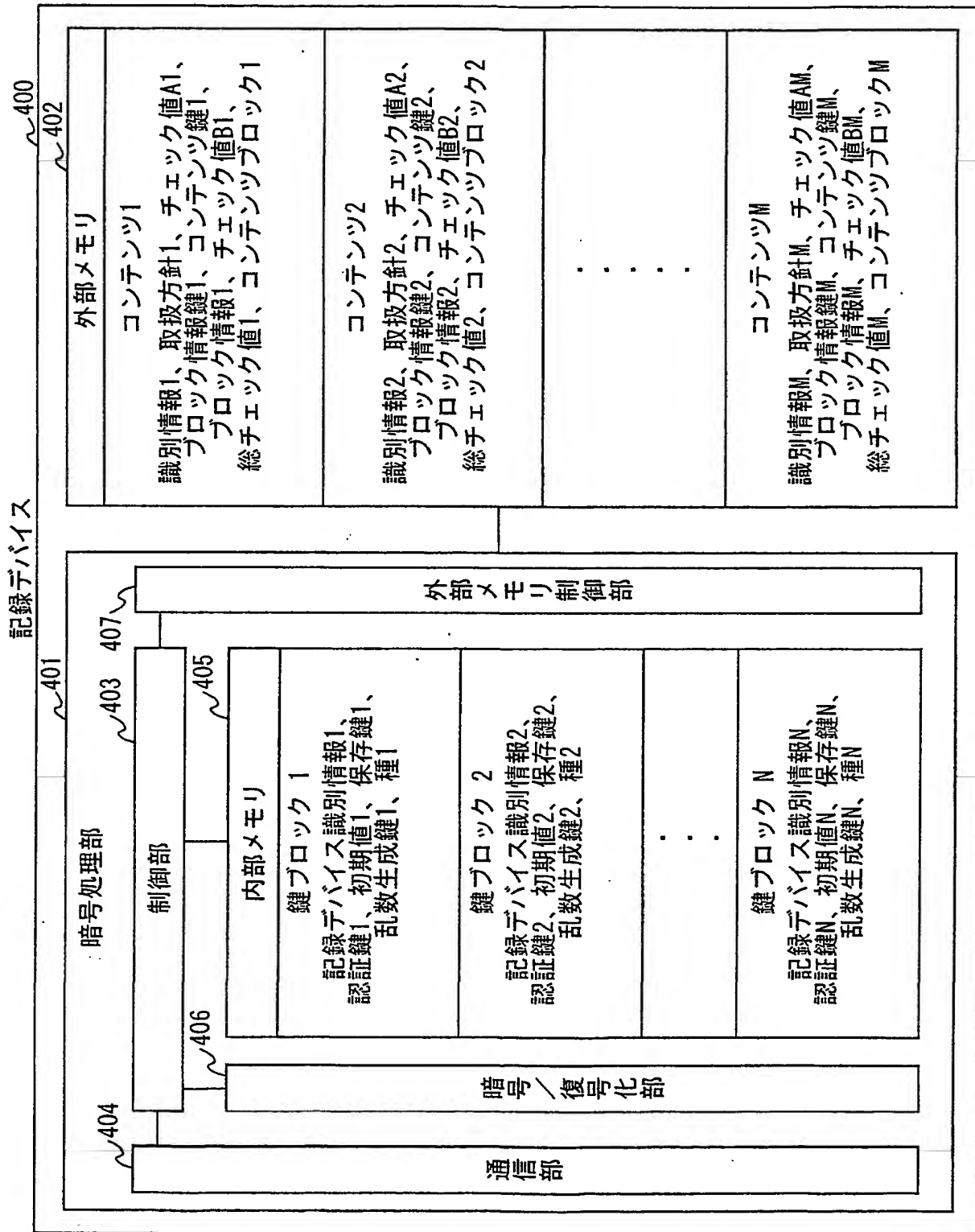
復号化楕円曲線暗号を用いた復号化 (Menezes-Vanstone)

図 1 7



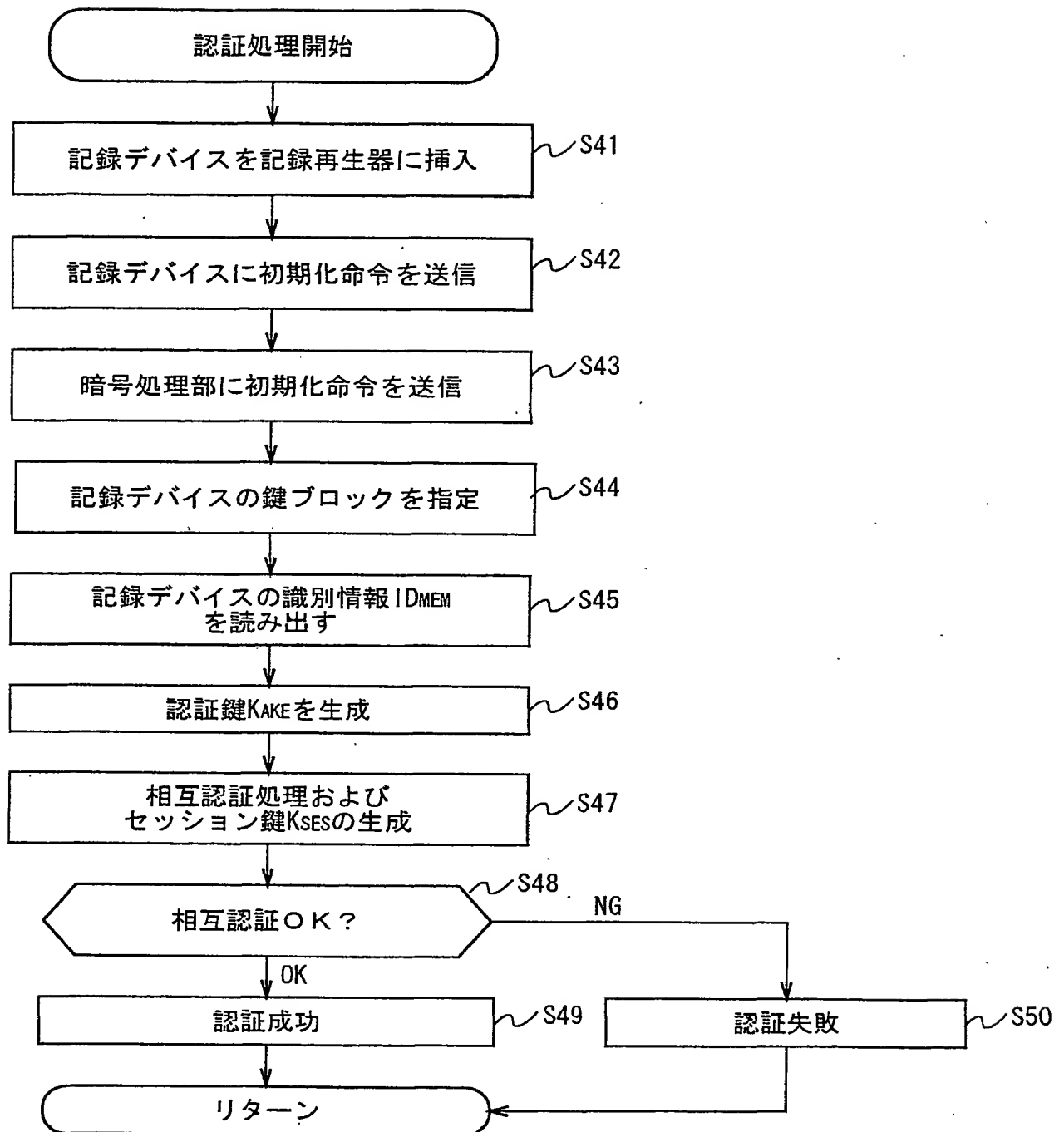
記録再生器上のデータ保持状況

図 18



記録デバイス上のデータ保持状況

図 19



記録再生器と記録デバイスとの相互認証

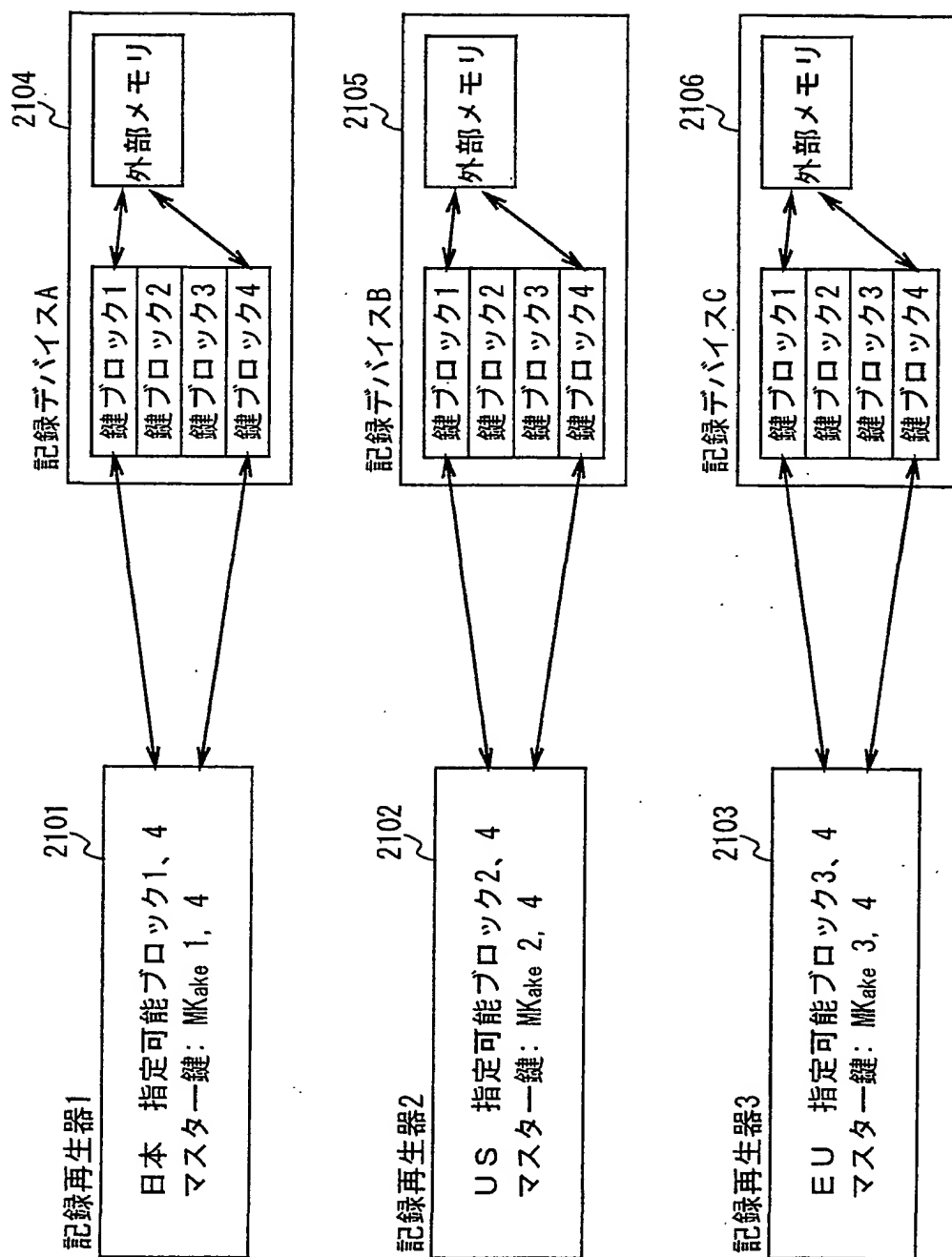


図 2 1.

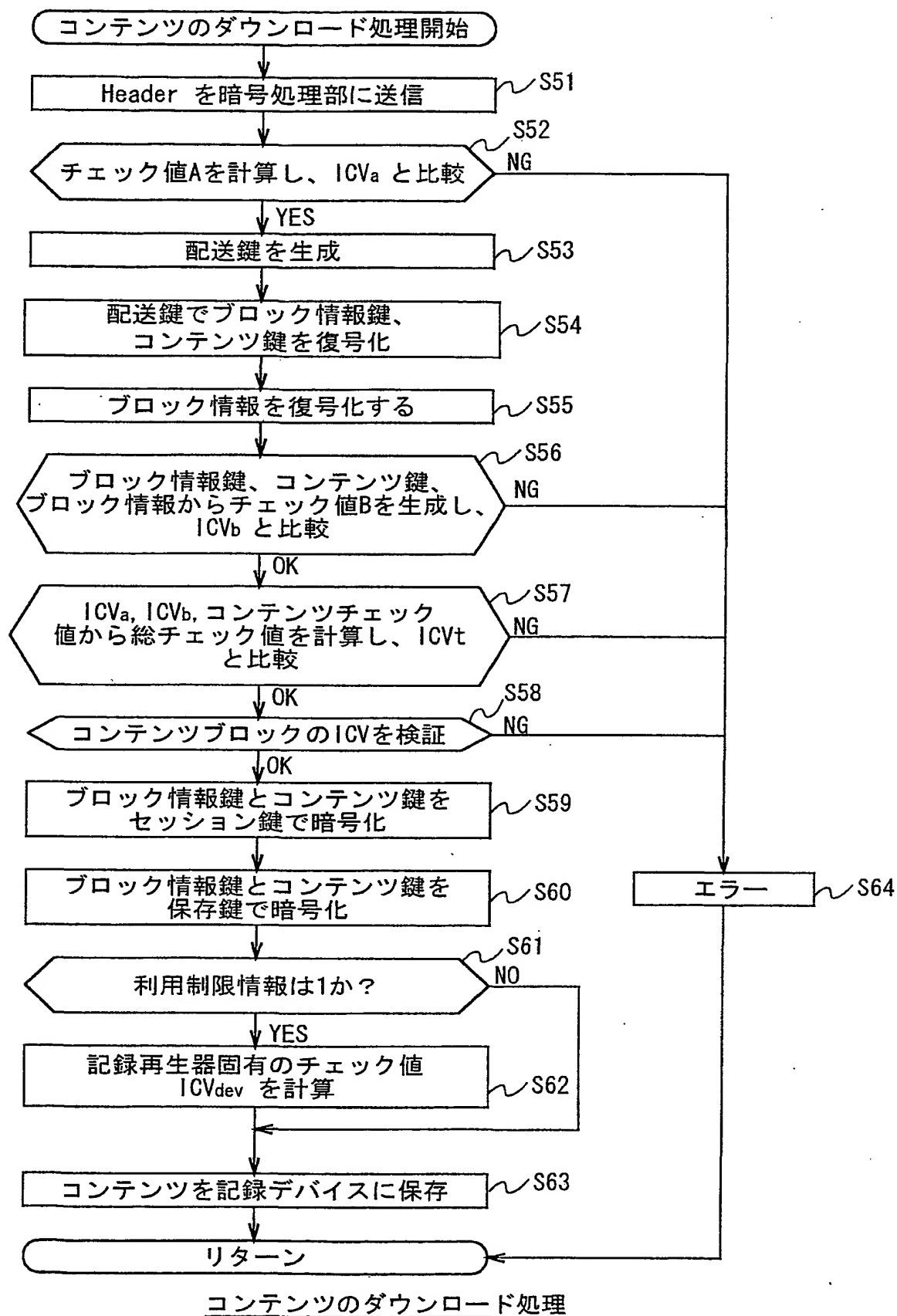


図 2 2

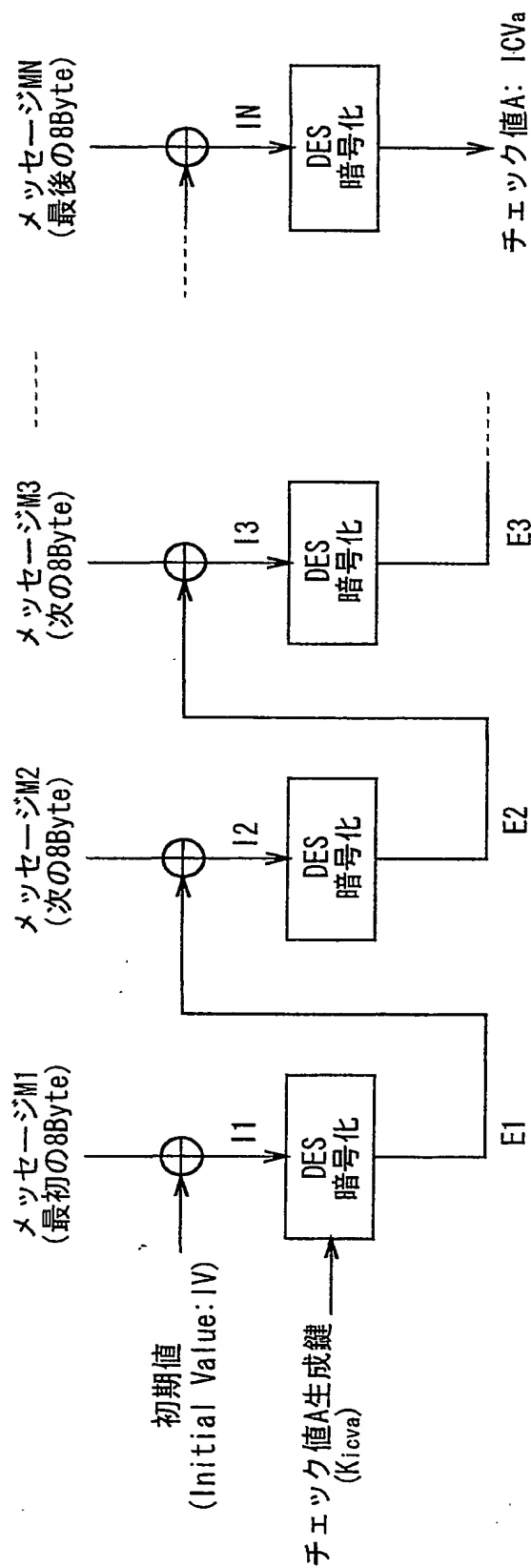
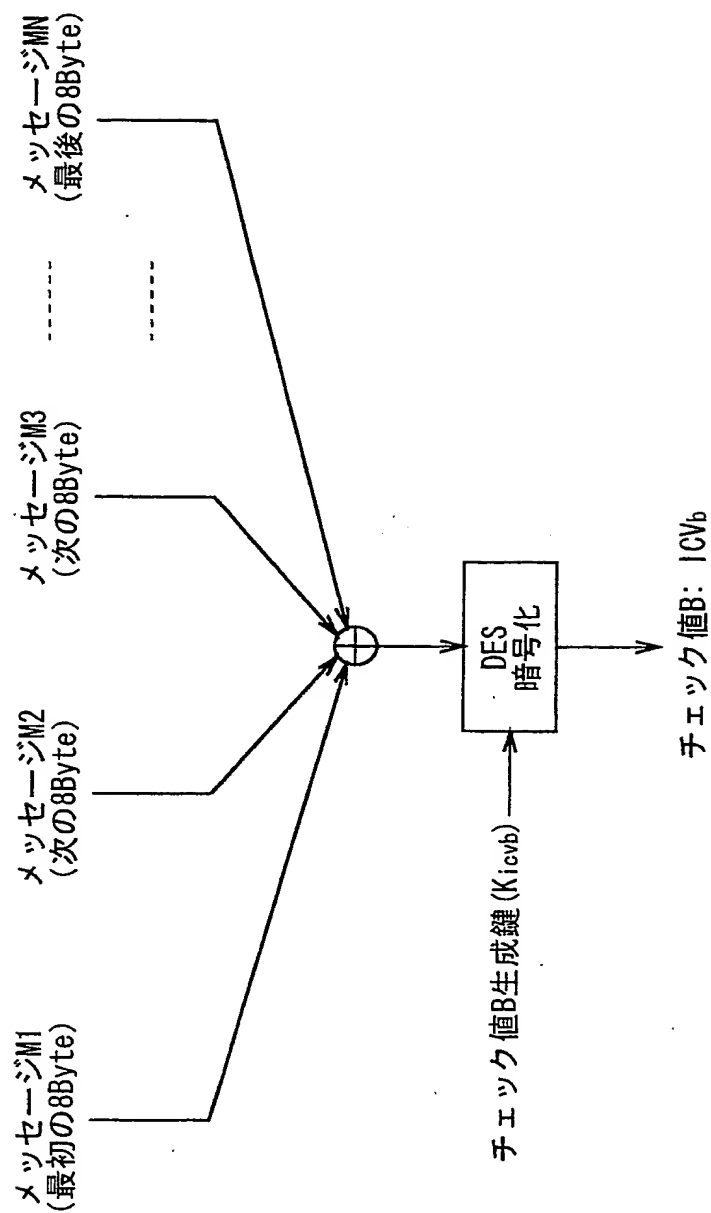


図 23

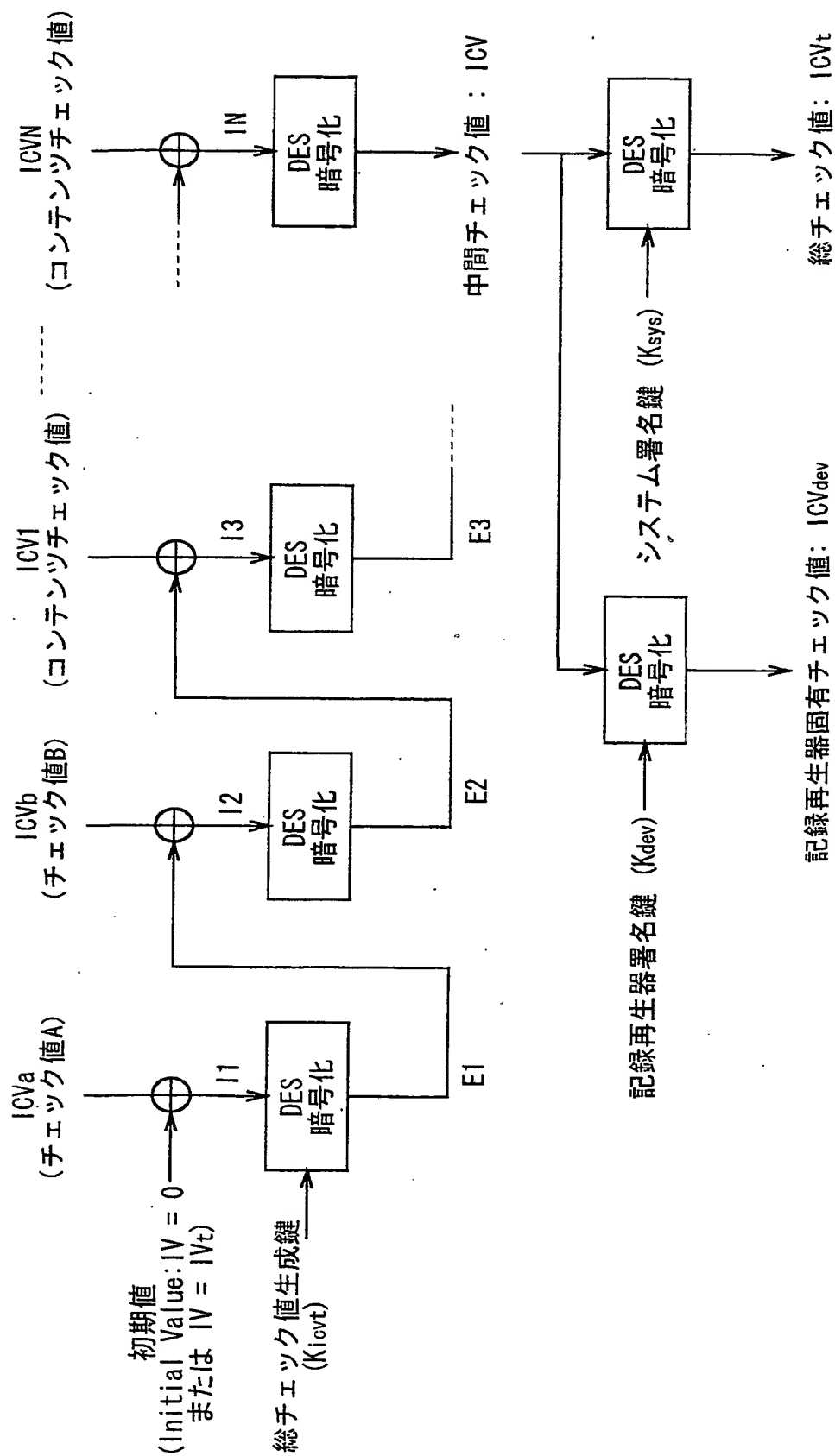
メッセージM1～MN:識別情報、取扱方針

⊕:排他的論理和処理 (8バイト単位)



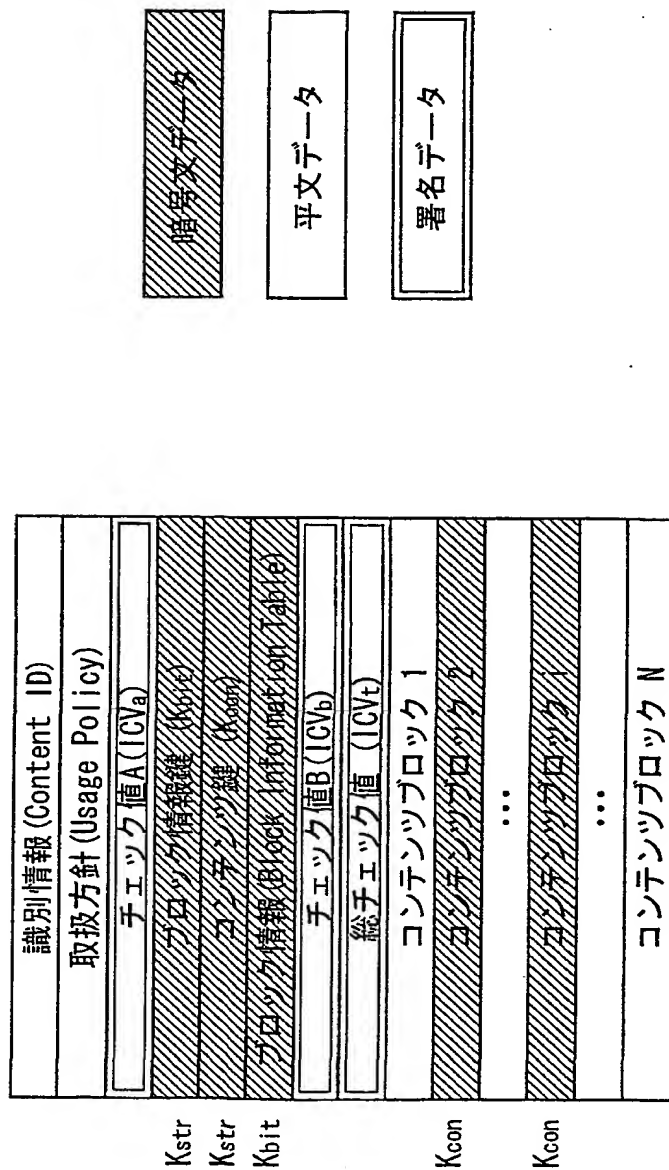
メッセージM1～MN : ブロック情報鍵 K_{bit} , コンテンツ鍵 K_{con} , ブロック情報
 ⊕: 排他的論理和処理 (8バイト単位)

図 24



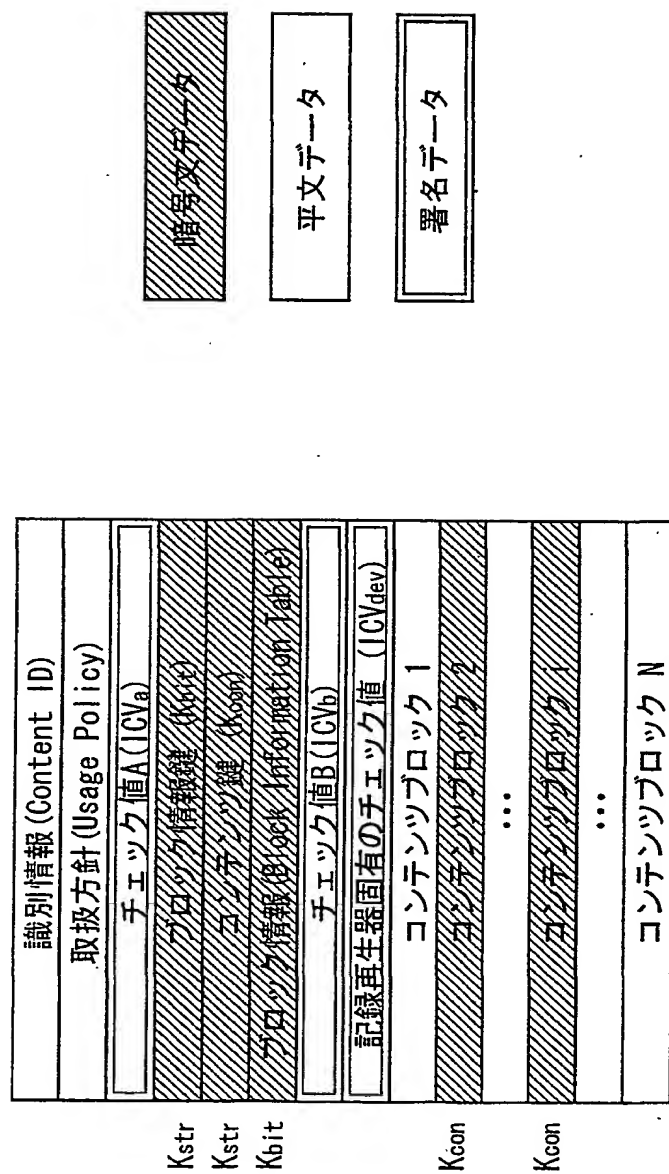
⊕: 排他的論理和処理 (8バイト単位)

図 25



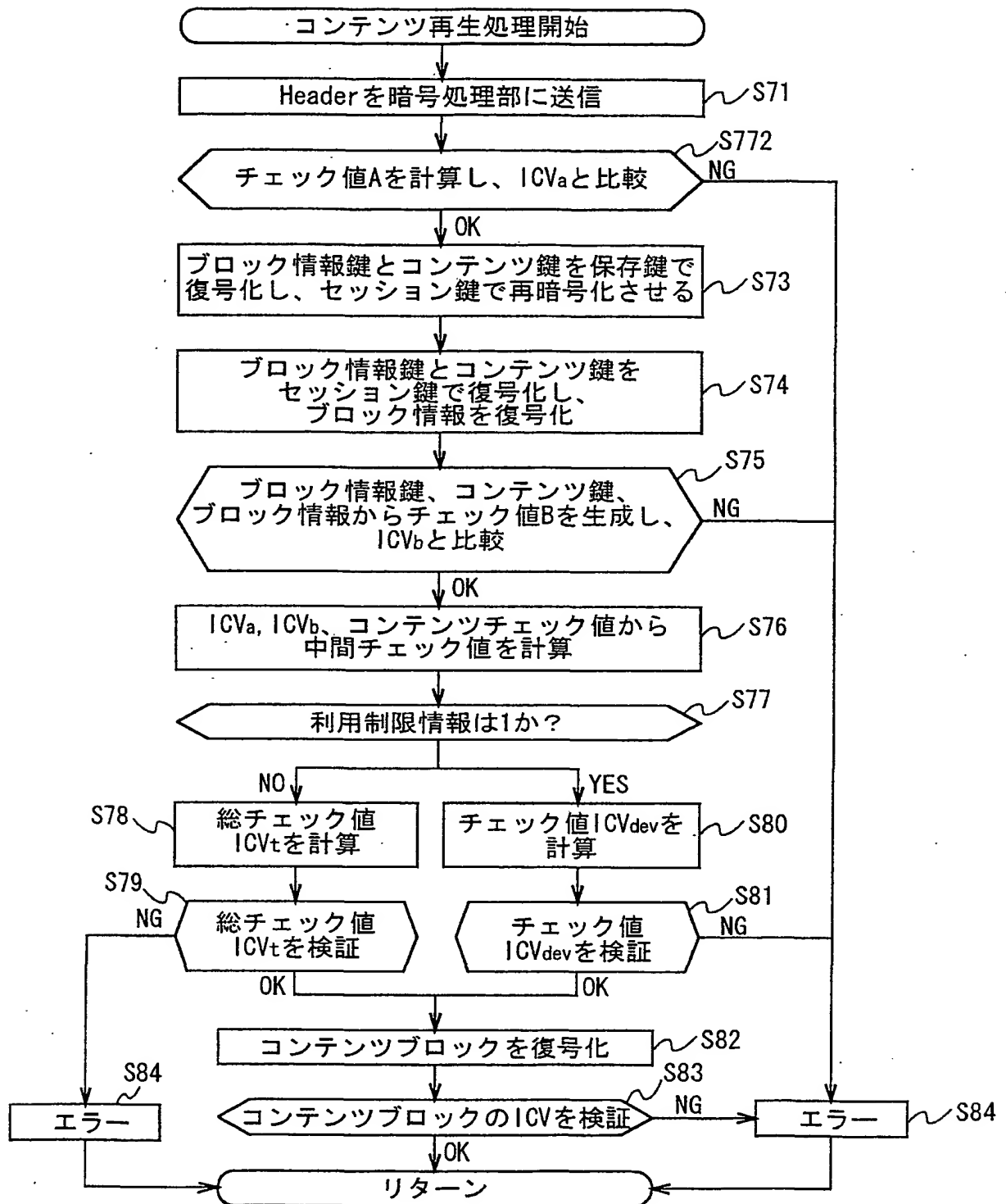
記録デバイスに保存されたコンテンツ
(記録制限情報 = 0)

図 26



記録デバイスに保存されたコンテンツ
(利用制限情報 = 1)

27



コンテンツの再生処理

図 2 8

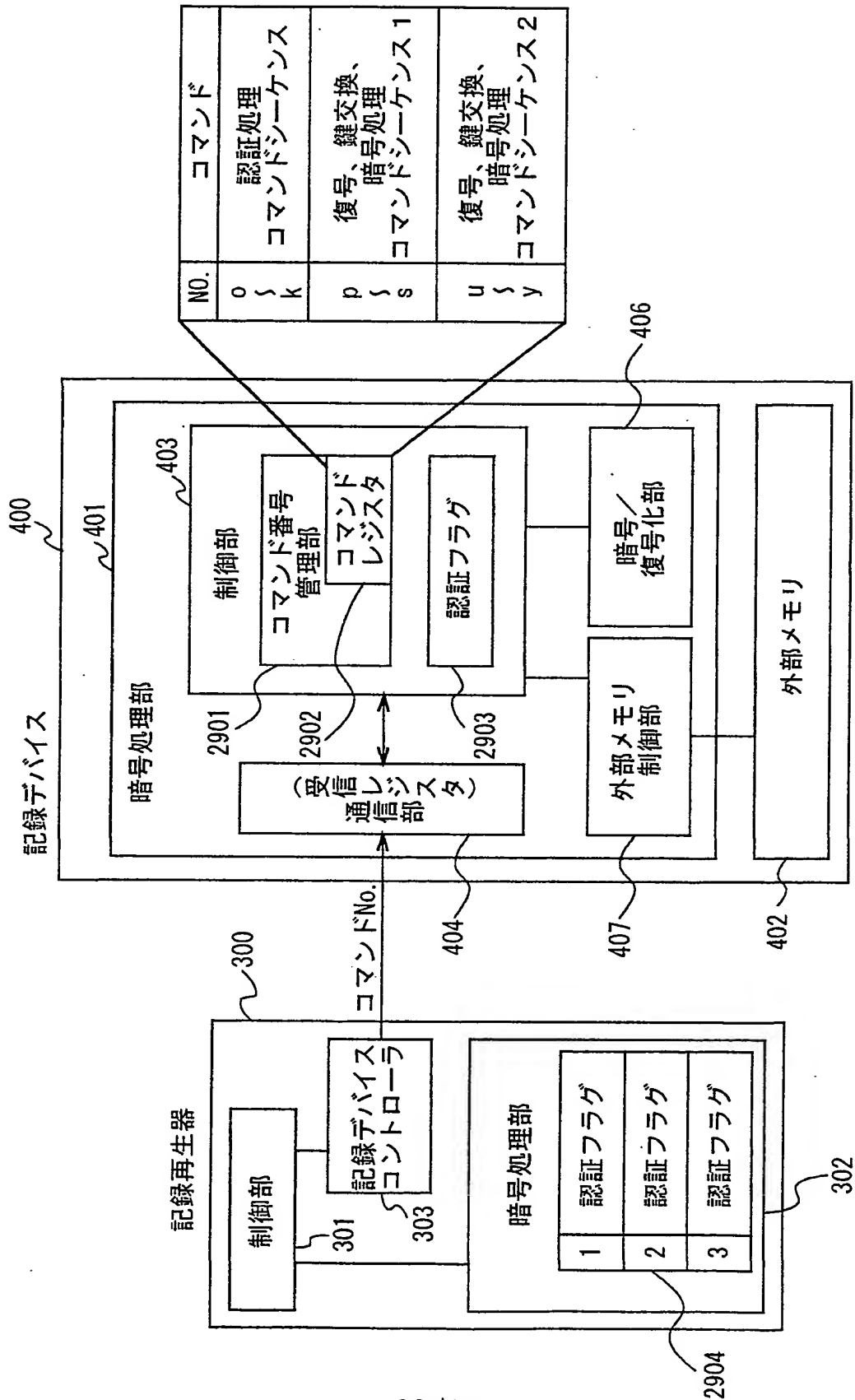


図 29

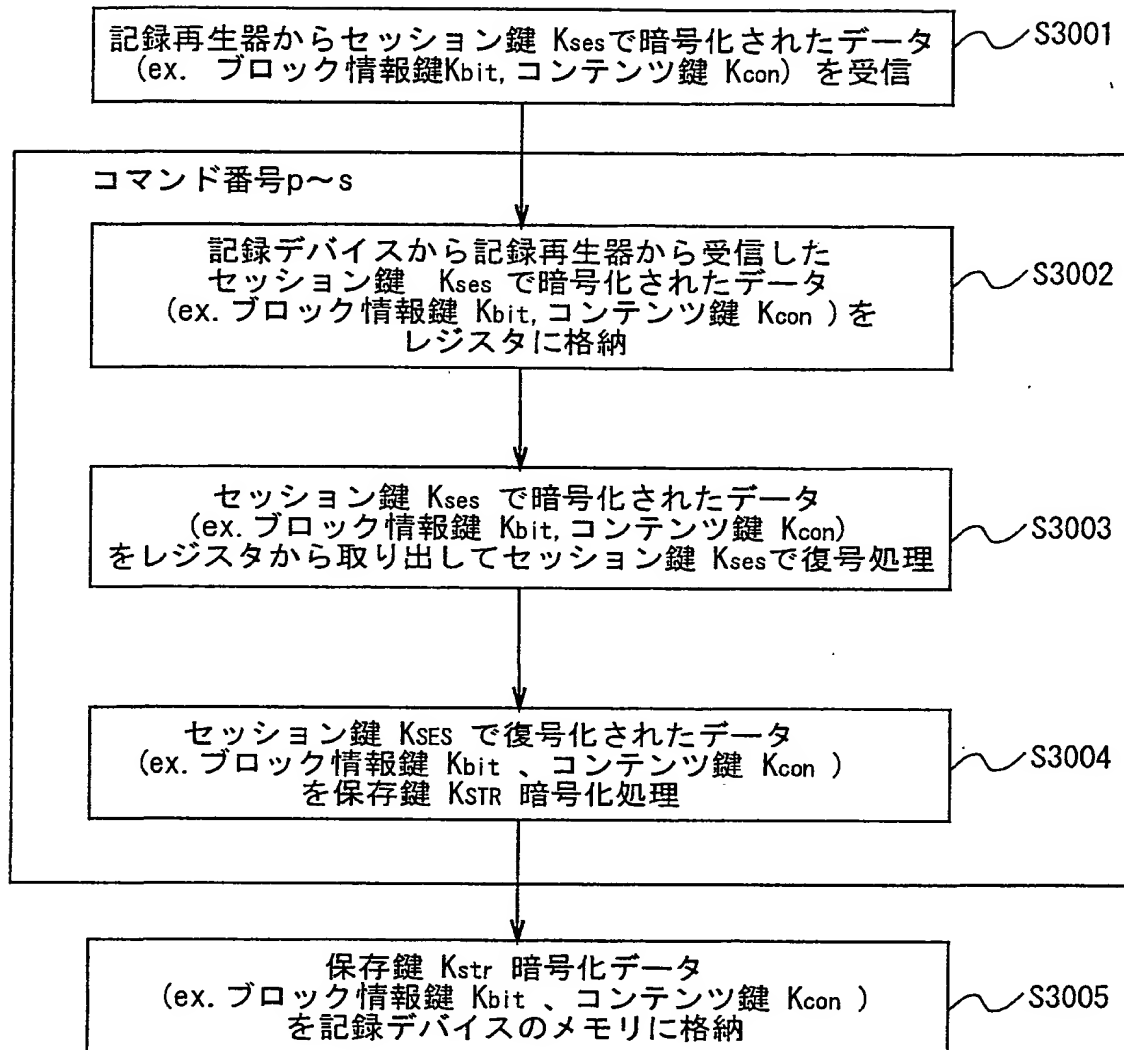


図 30

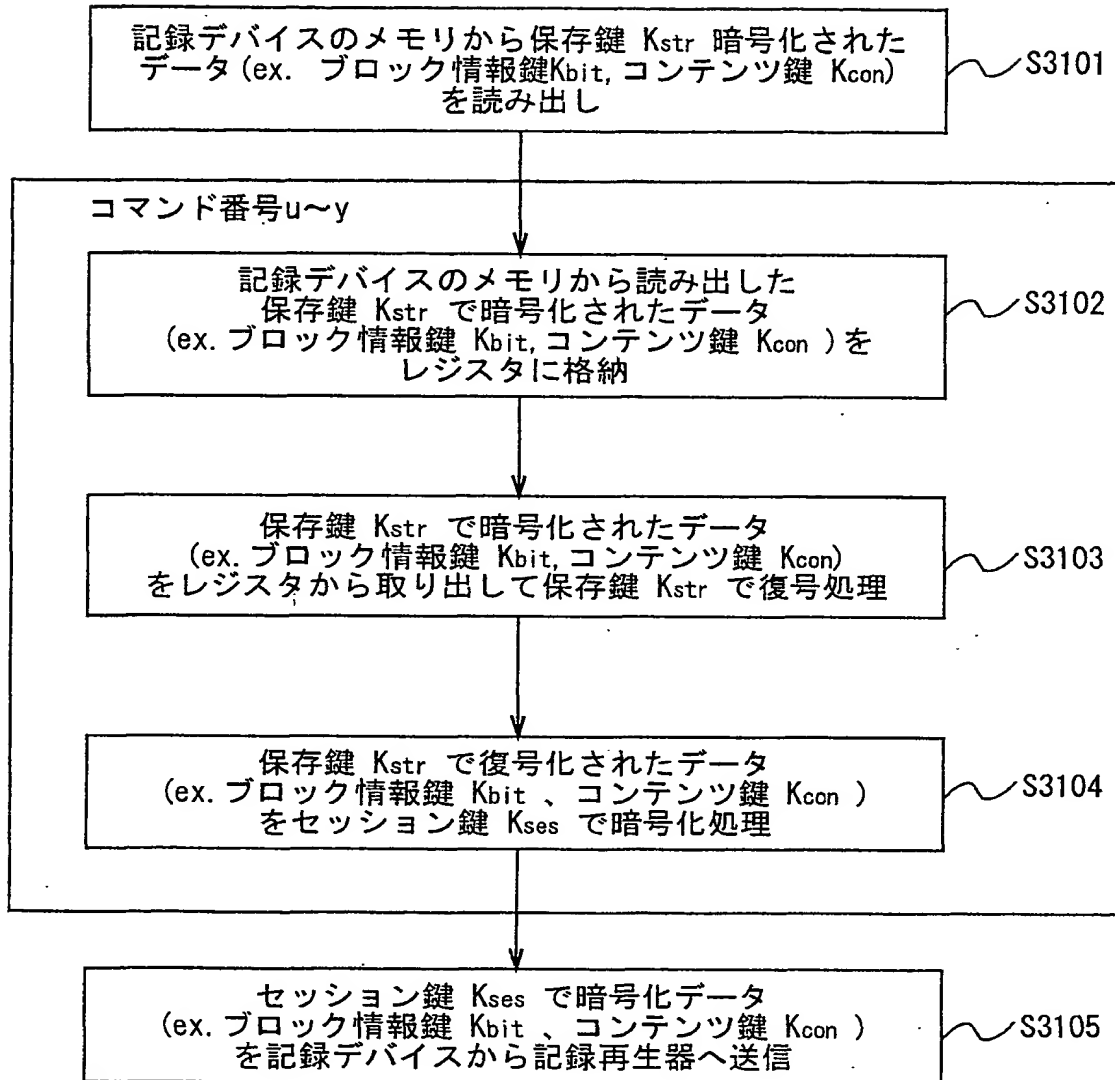


図 3 1

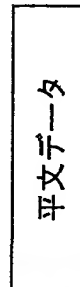
フォーマット・タイプ0

	識別情報 (CONTENT ID)
	取扱方針 (USAGE POLICY)
	チェック値A (ICV _a)
Kdis	ブロック情報鍵 (K _{bit})
Kdis	コンテンツ鍵 (K _{con})
Kbit	ブロック情報 (BLOCK INFORMATION TABLE)
	チェック値B (ICV _b)
	総チェック値 (ICV _t)
	コンテンツブロック1
Kcon	コンテンツブロック2
	...
Kcon	コンテンツブロックN
	...
	コンテンツブロックN

メディア上及び通信路上のデータフォーマット



暗号化データ



平文データ



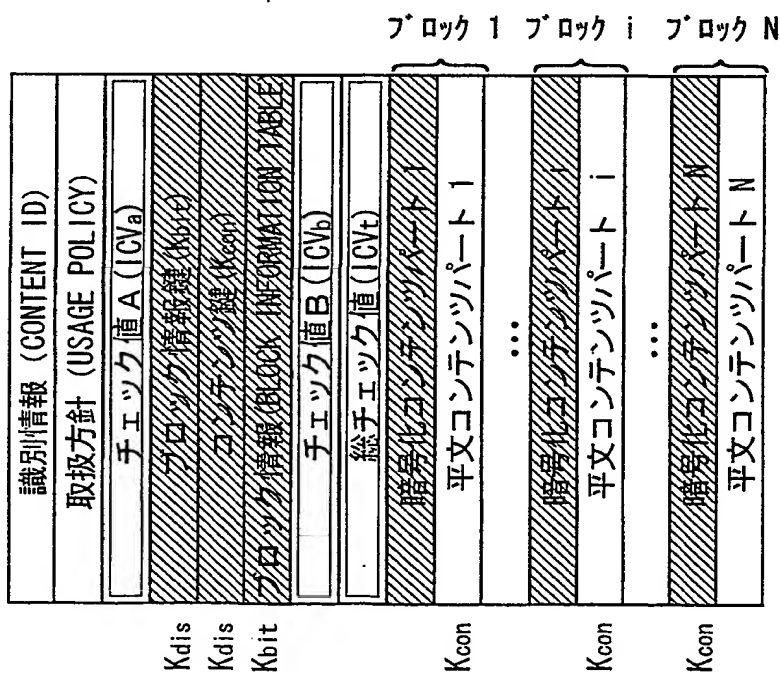
署名データ

図32

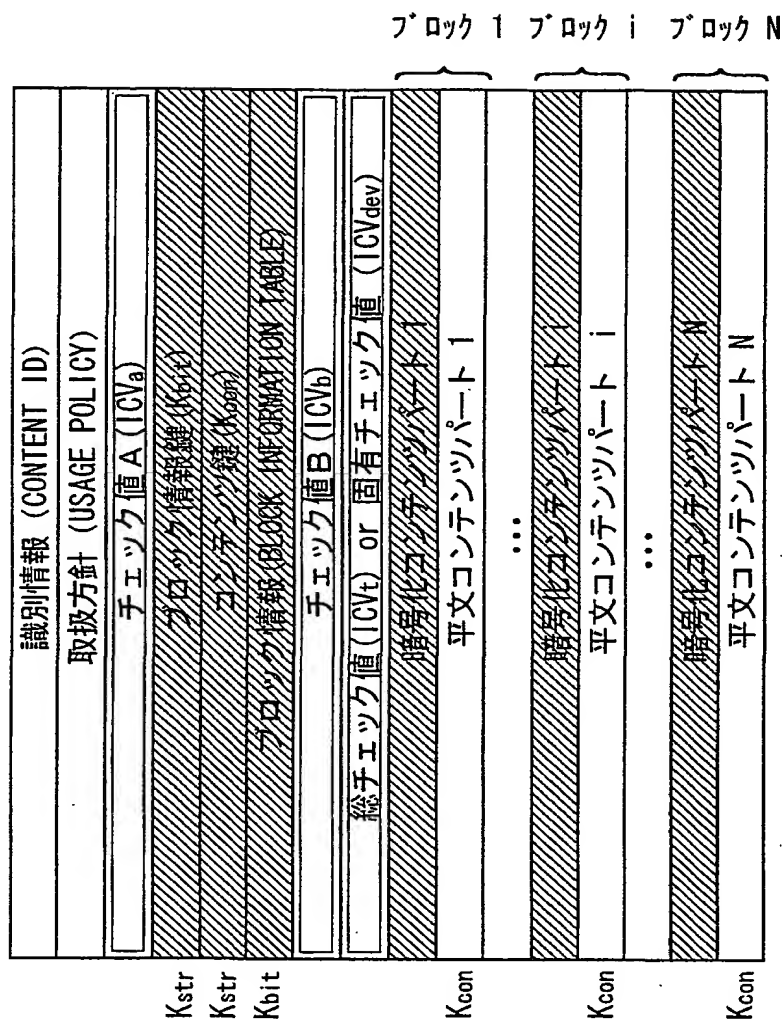
	識別情報 (CONTENT ID)
	取扱方針 (USAGE POLICY)
	チェック値A (ICV _a)
Kstr	ブロック情報鍵 (K _{bit})
Kstr	コンテンツ鍵 (K _{con})
Kbit	ブロック情報 (BLOCK INFORMATION TABLE)
	チェック値B (ICV _b)
	総チェック値 (ICV _t) or 固有チェック値 (ICV _{dev})
	コンテンツブロック1
Kcon	コンテンツブロック2
	...
Kcon	コンテンツブロックN
	...
	コンテンツブロックN

記録デバイスに保存されたコンテンツ

フォーマット・タイプ 1



メディア上及び通信路上のデータフォーマット



記録デバイスに保存されたコンテンツ

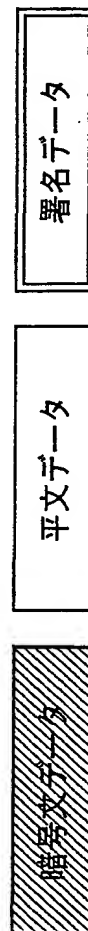
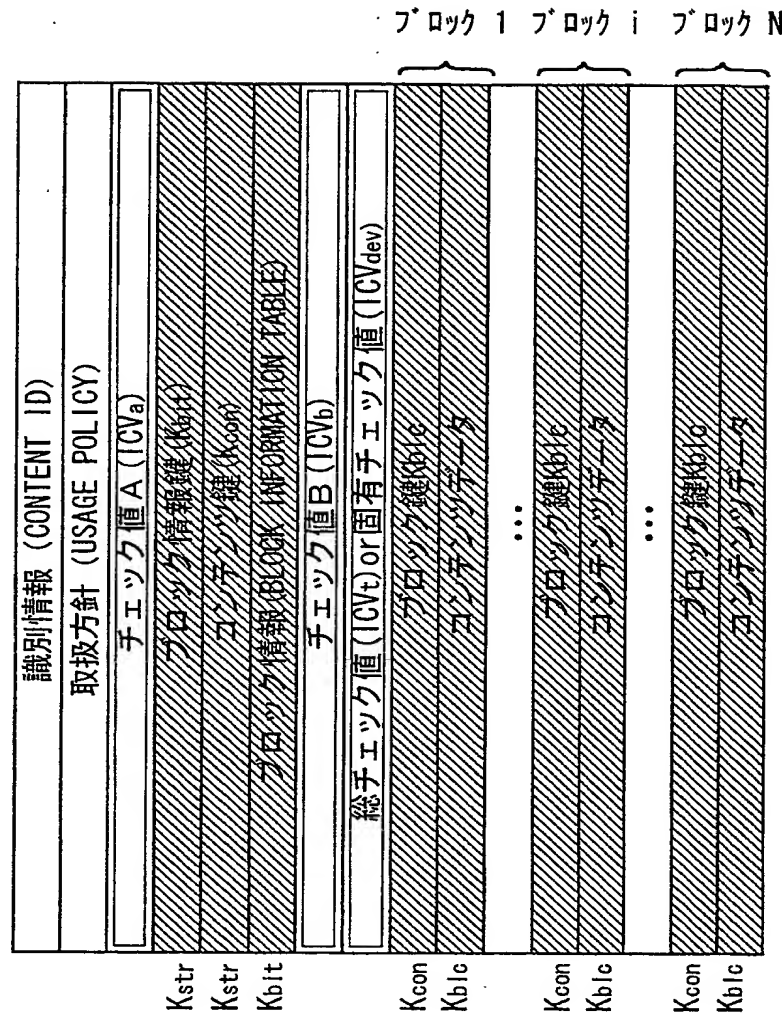
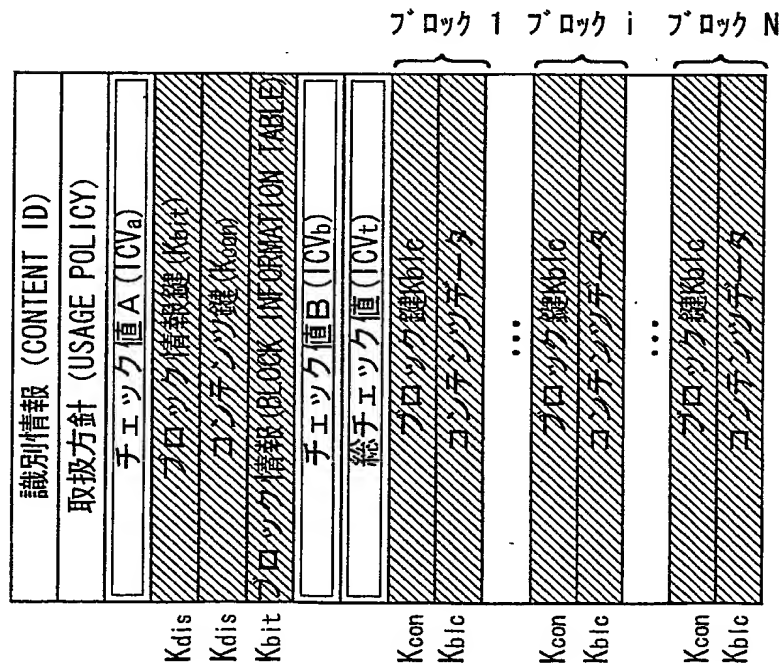


図 33

フォーマット・タイプ2



メディア上及び通信路上のデータフォーマット

記録デバイスに保存されたコンテンツ

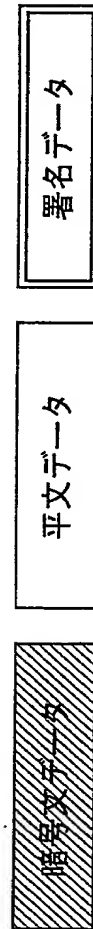
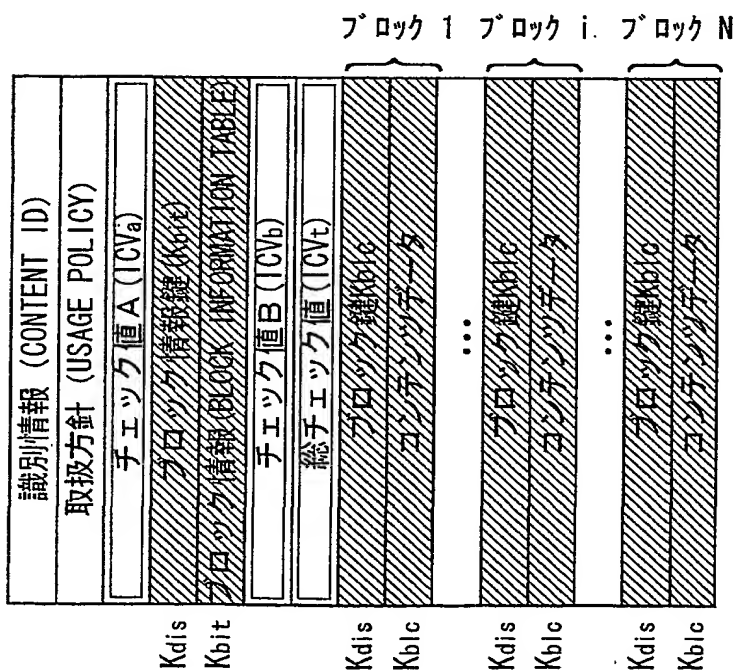


図34

フォーマット・タイプ3

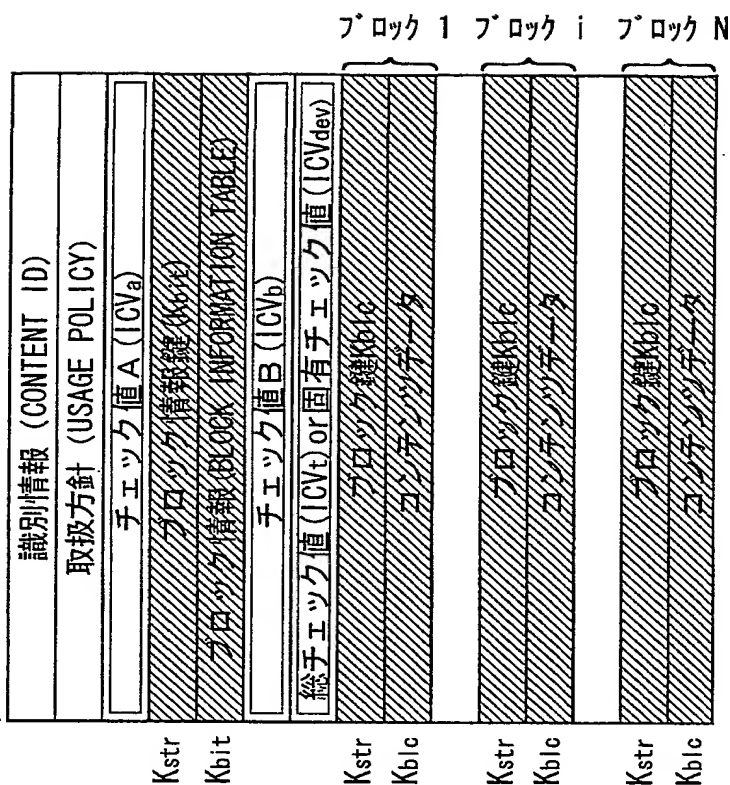


メディア上及び通信路上のデータフォーマット



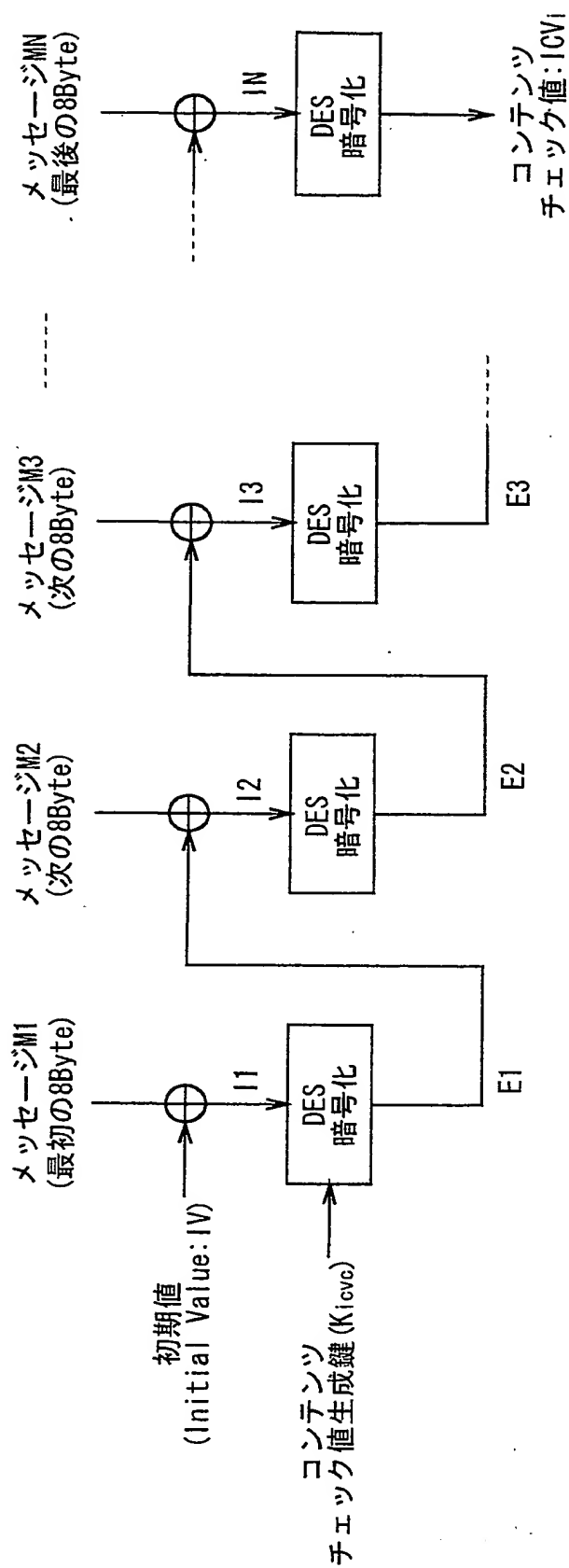
署名データ

署名データ



記録デバイスに保存されたコンテンツ

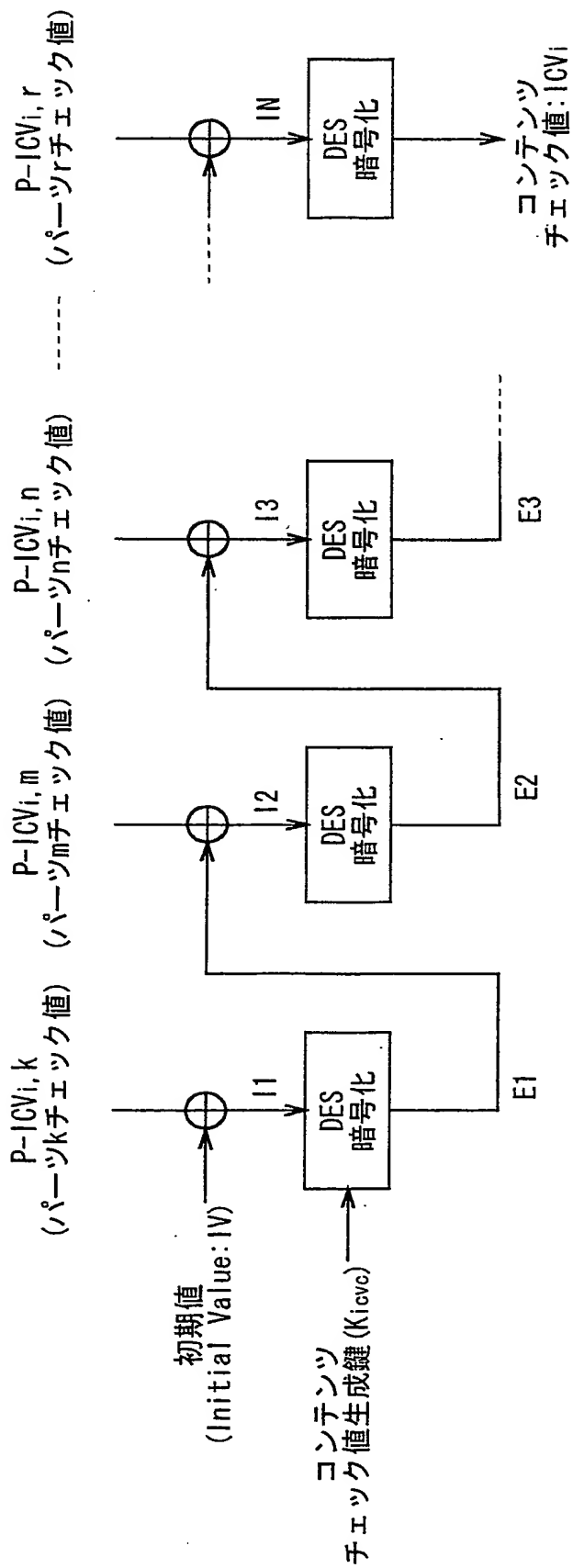
図 35



メッセージM1～MN: コンテンツiのコンテンツデータ

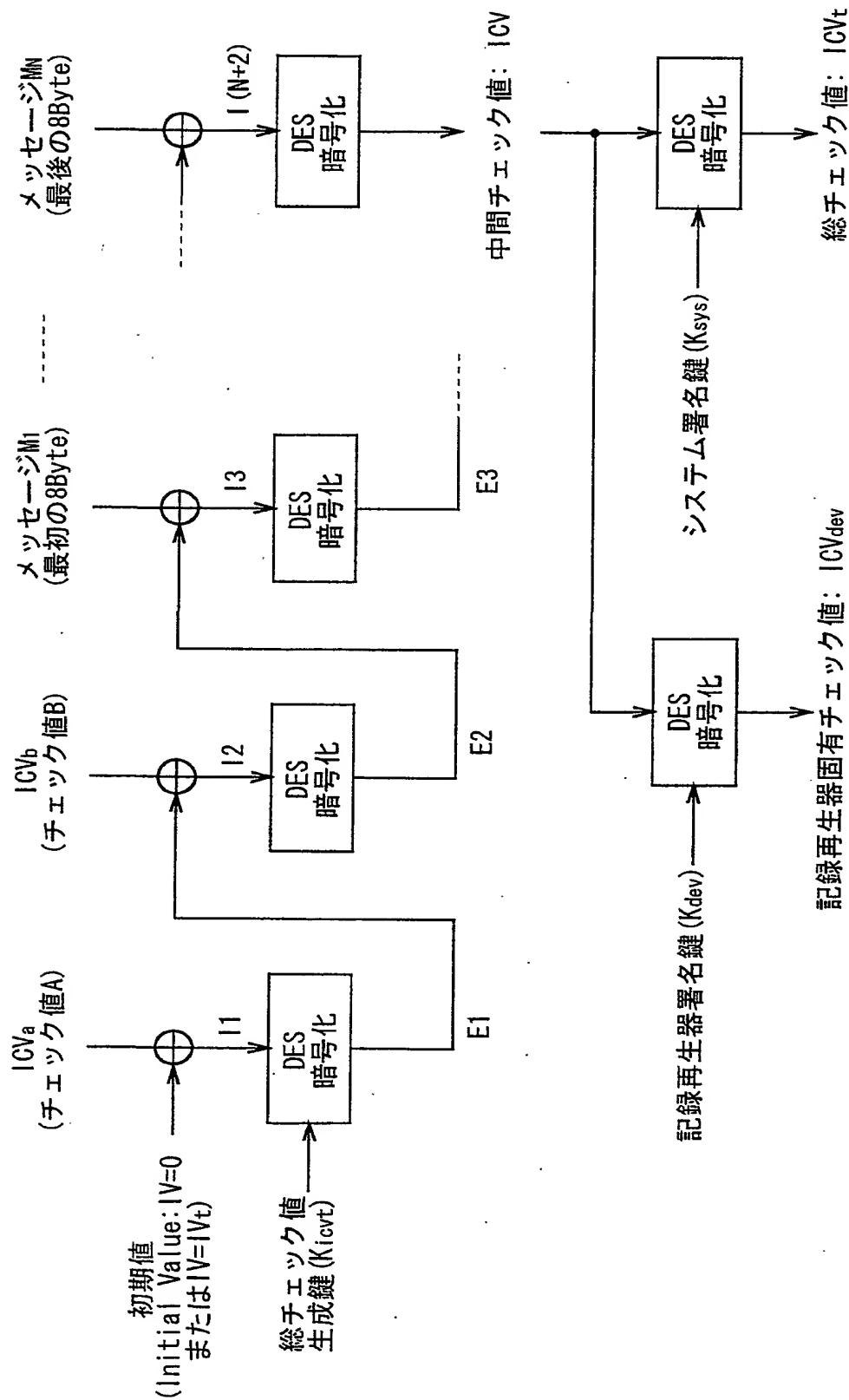
⊕: 排他的論理和処理 (8バイト単位)

図 3 6



⊕: 排他的論理和処理 (8バイト単位)

図 37

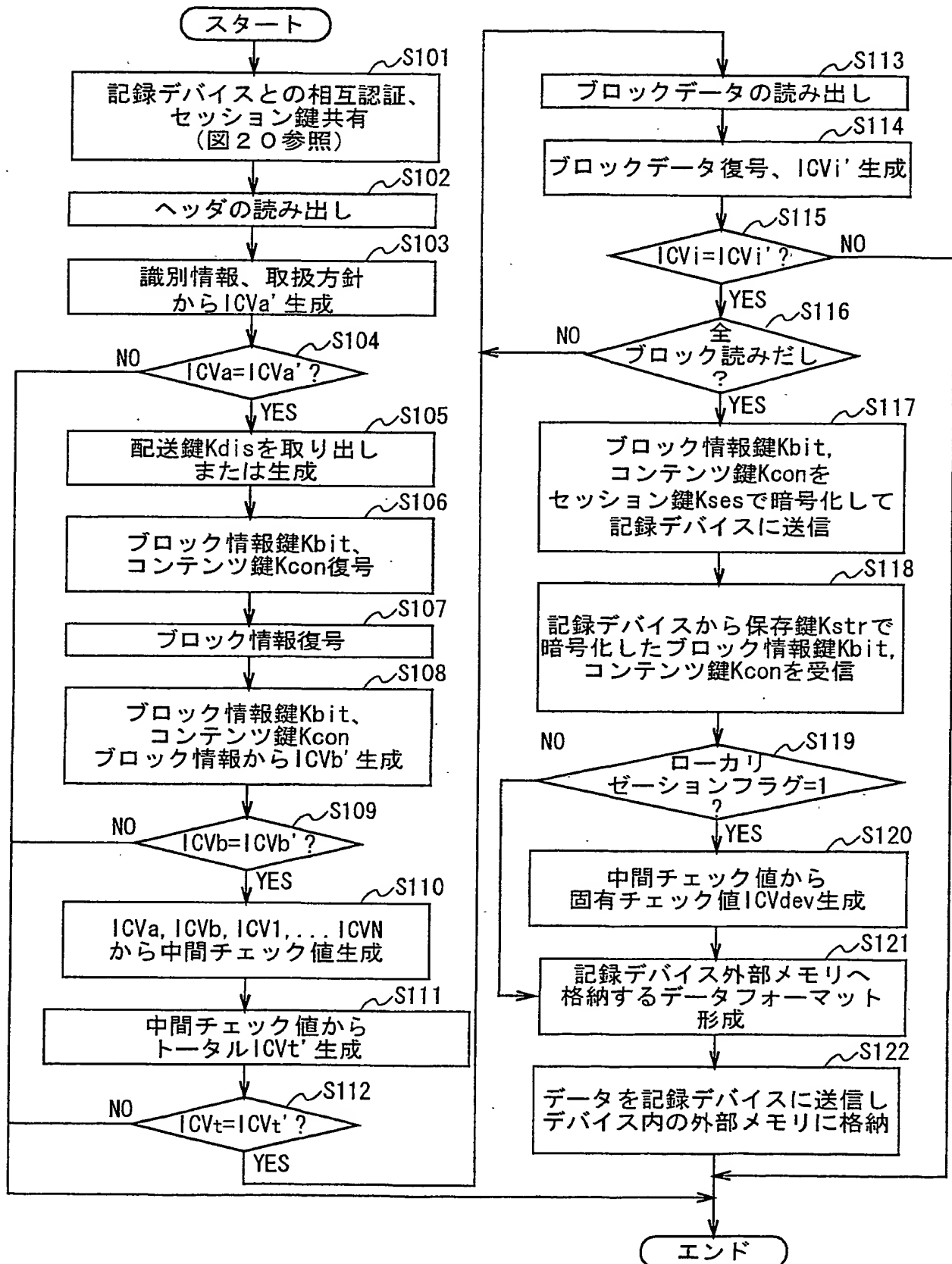


メッセージM1～MN: コンテンツブロック1～Nのデータ

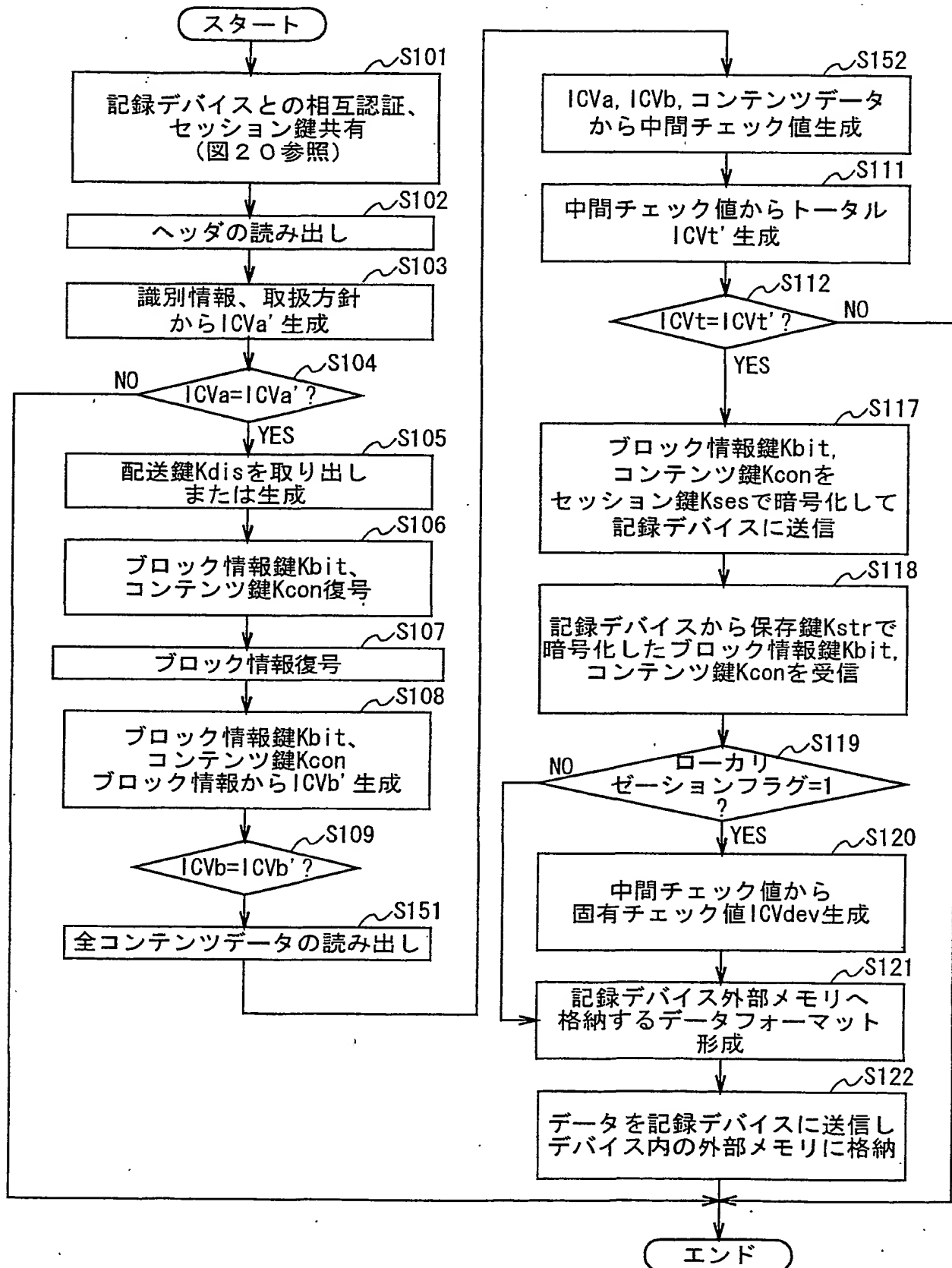
⊕: 排他的論理和処理 (8バイト単位)

図 38

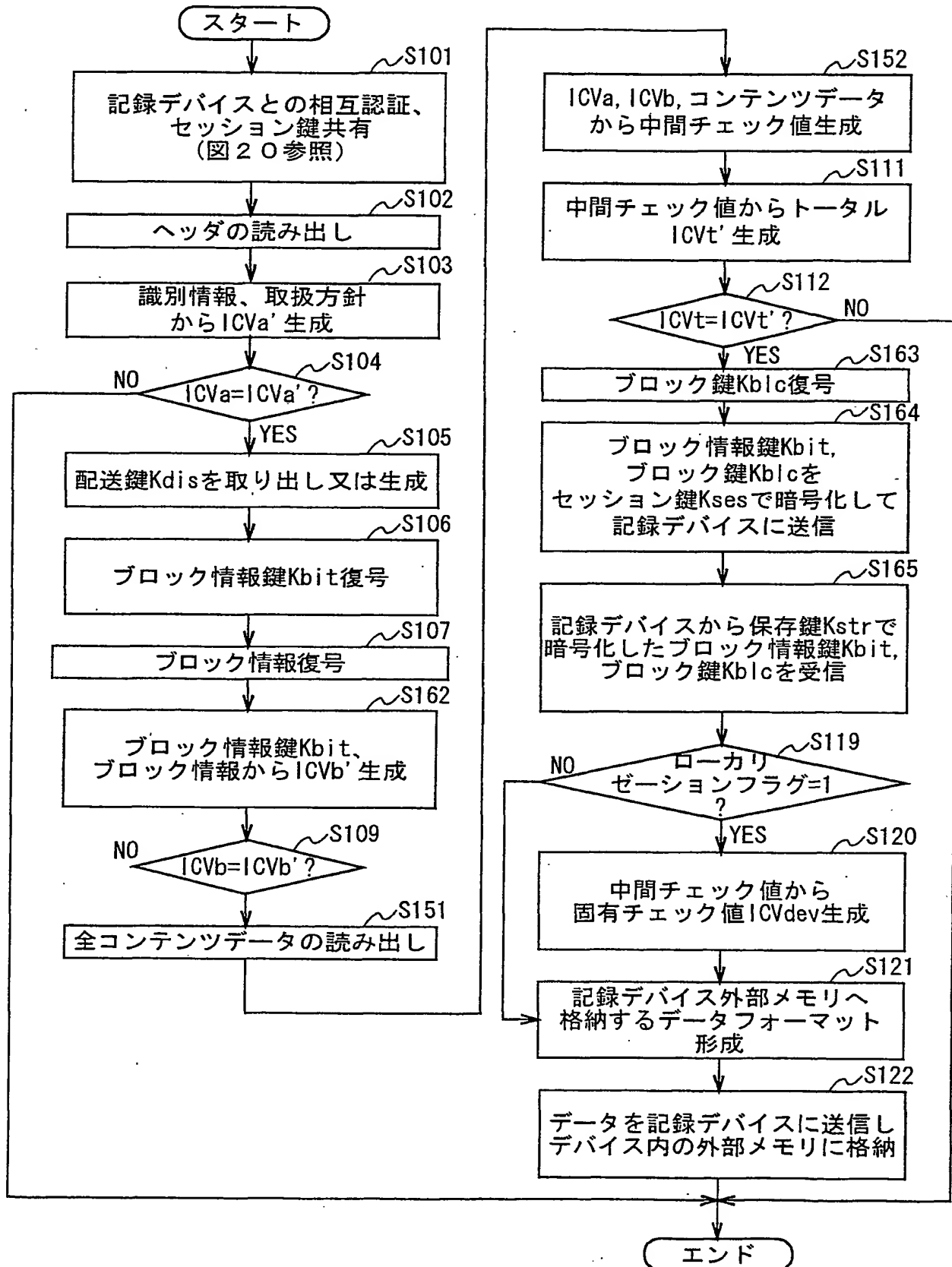
フォーマットタイプ0, 1ダウンロード処理



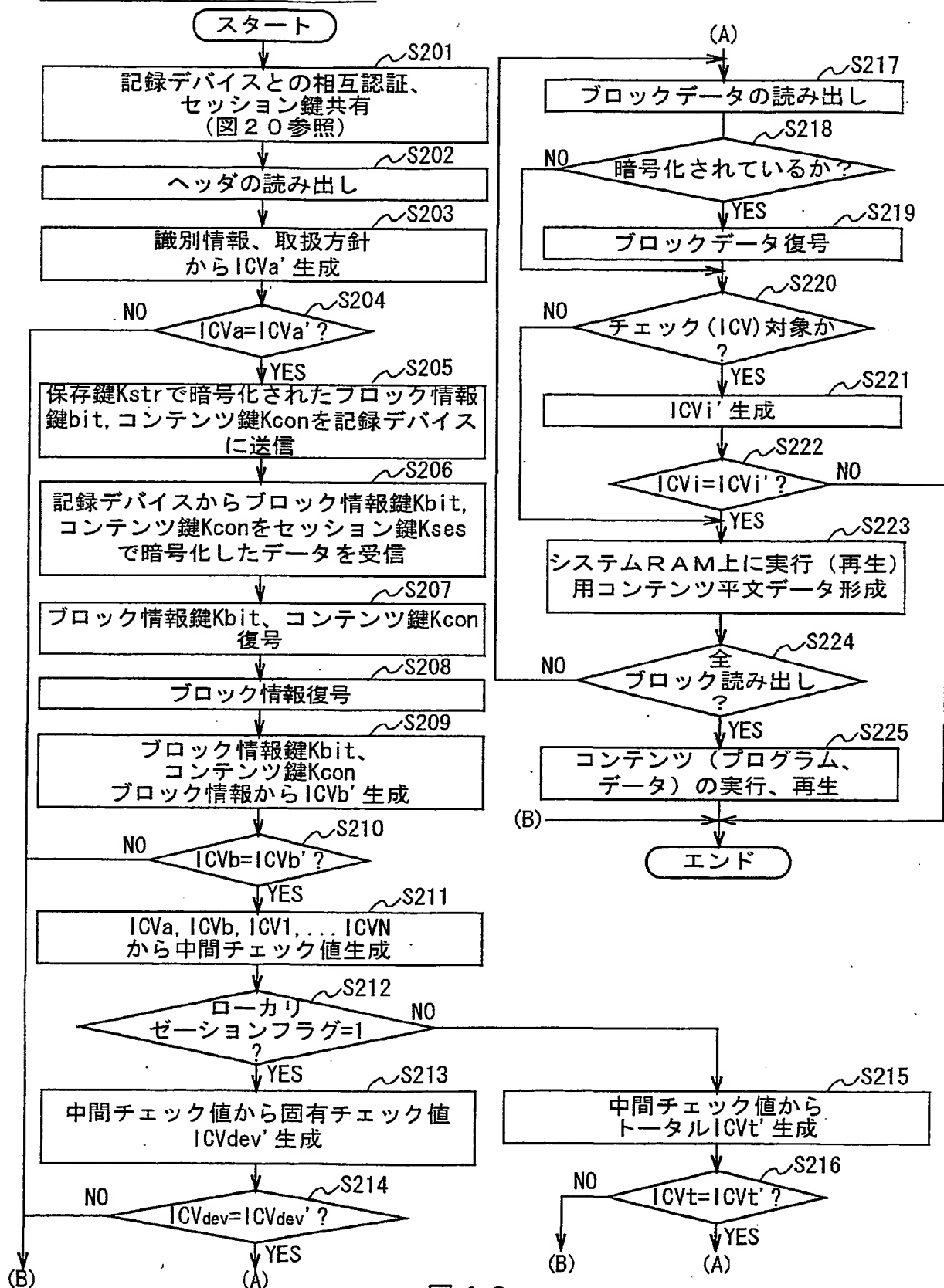
フォーマットタイプ2 ダウンロード処理

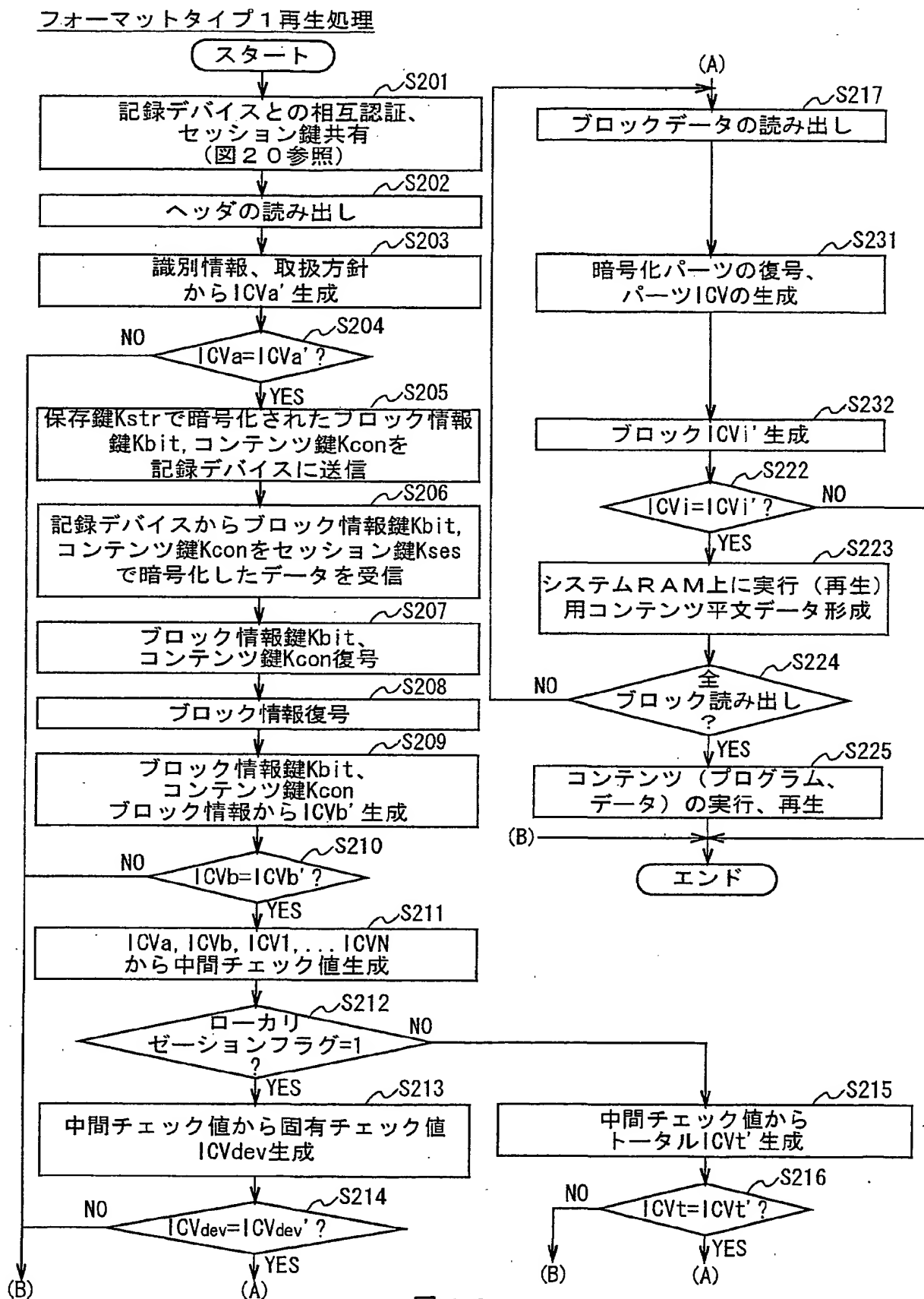


フォーマットタイプ3ダウンロード処理



フォーマットタイプ0再生処理





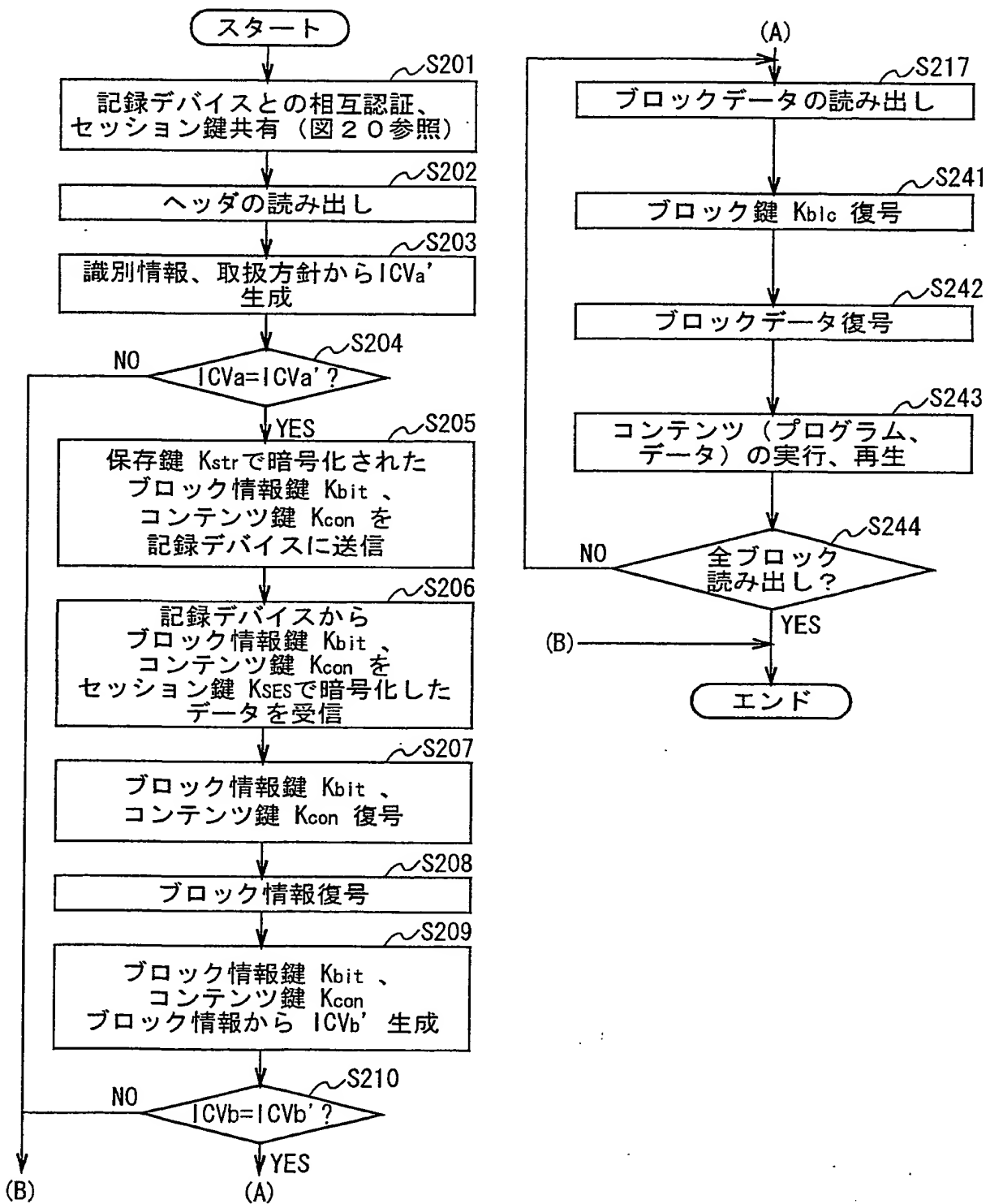


図 4 4

フォーマットタイプ3再生処理

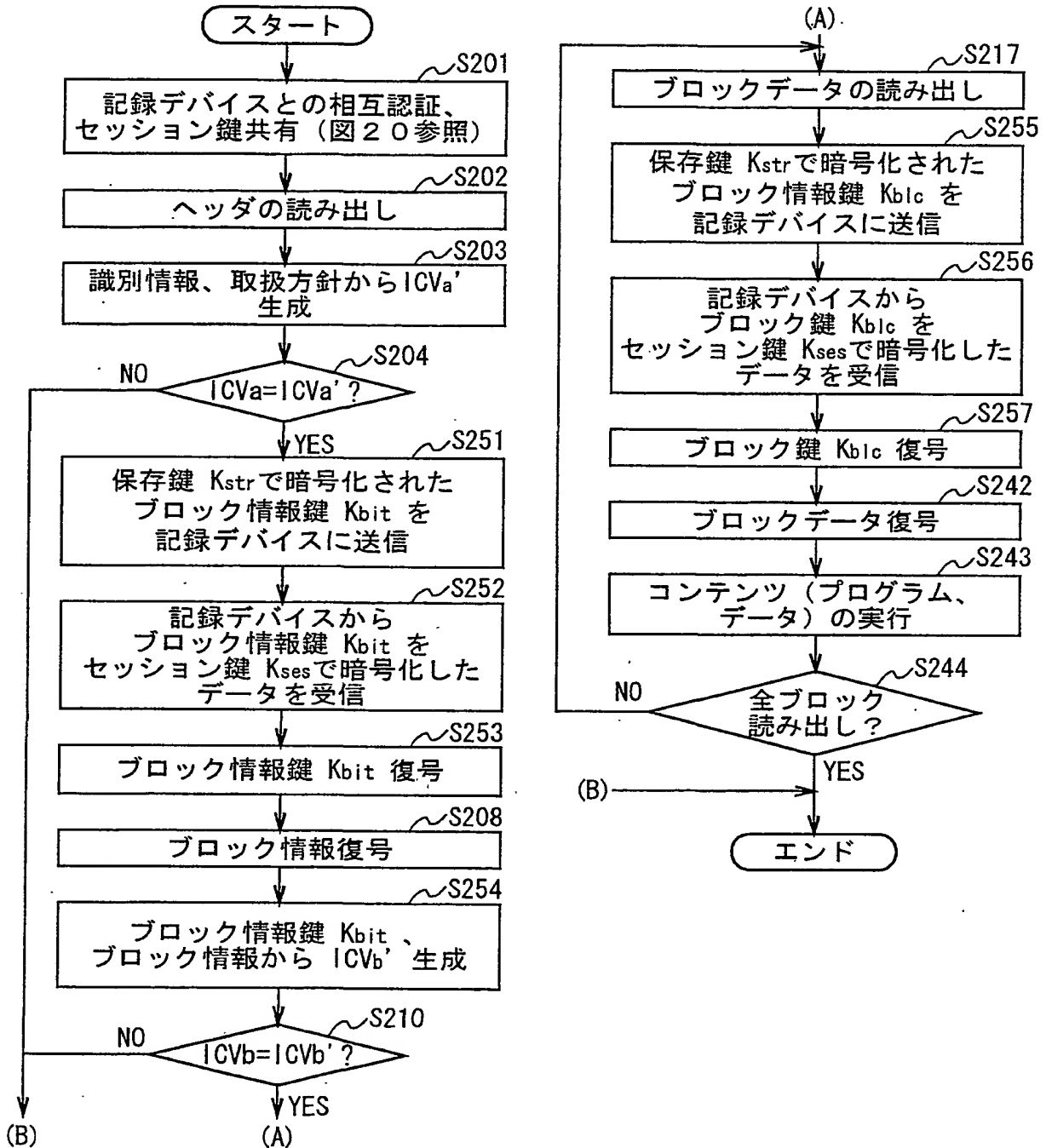


図 4 5

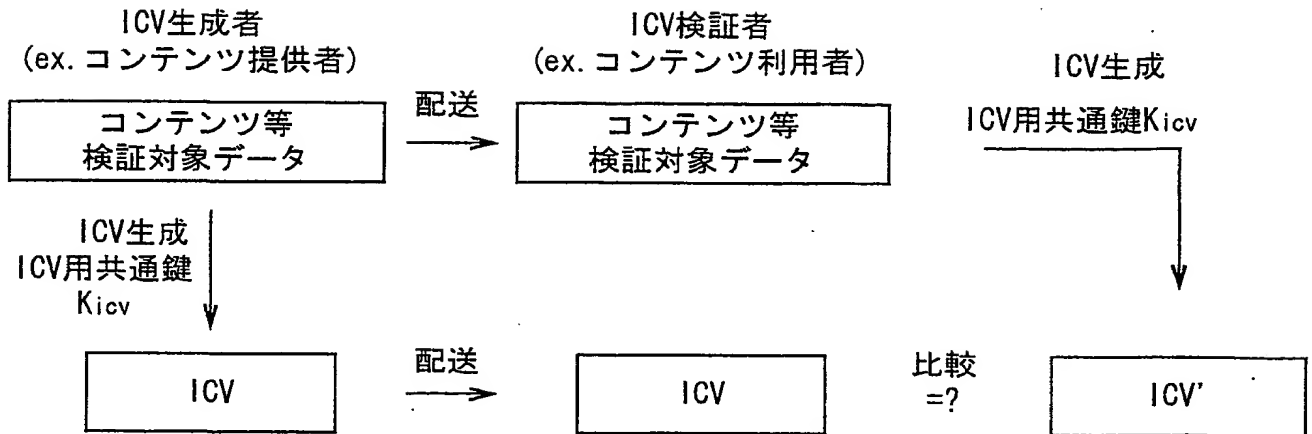


図 4 6

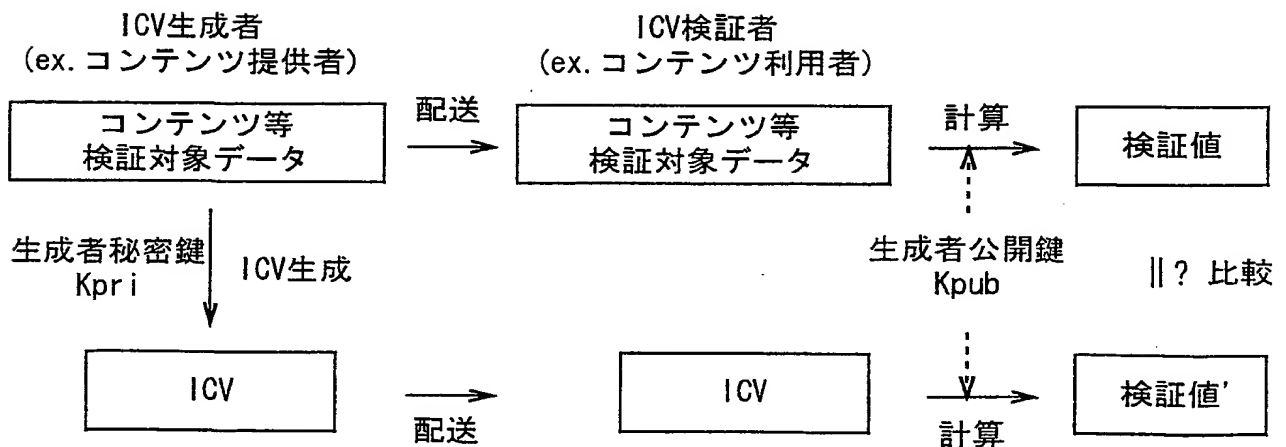


図 4 7

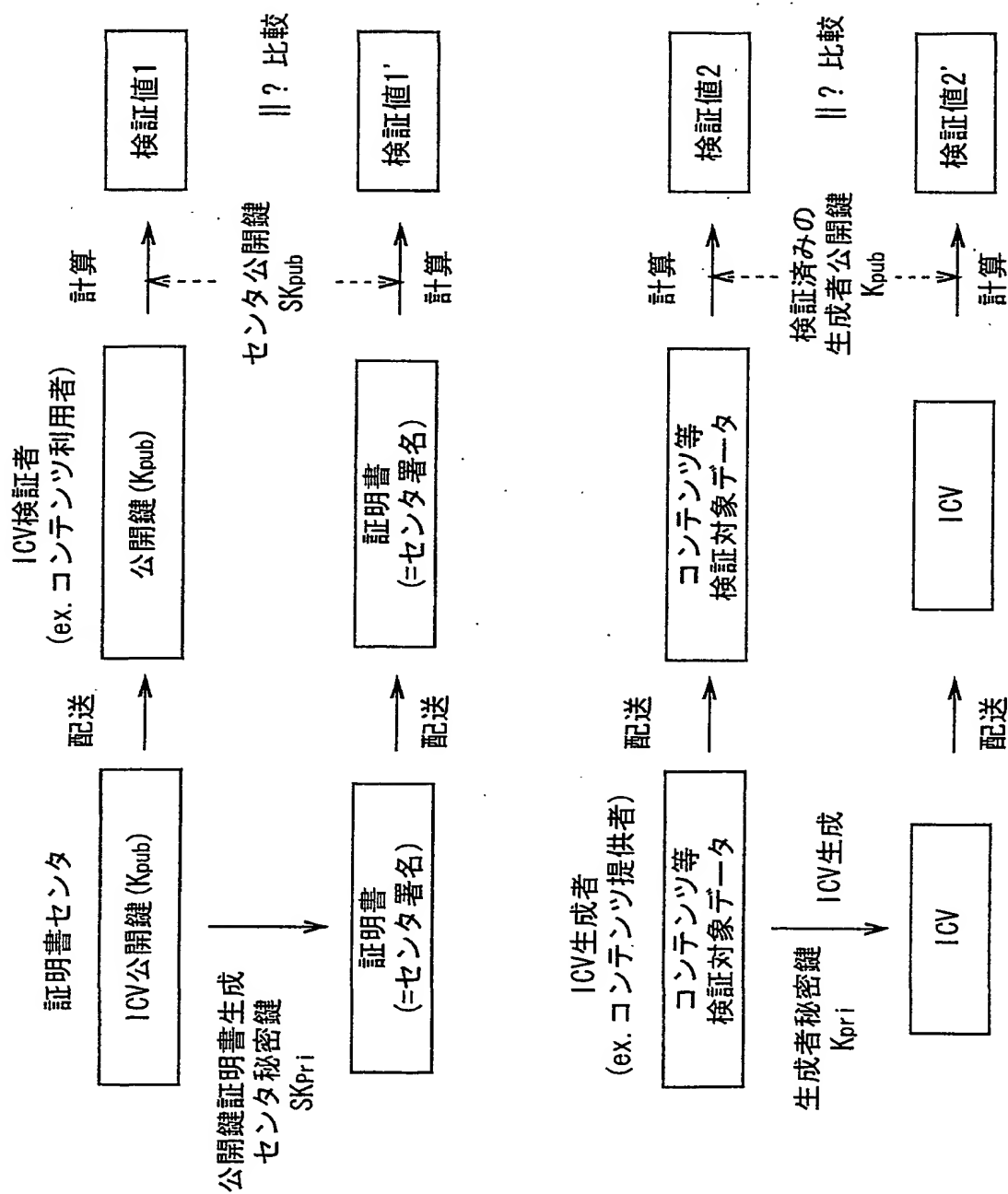


図 48

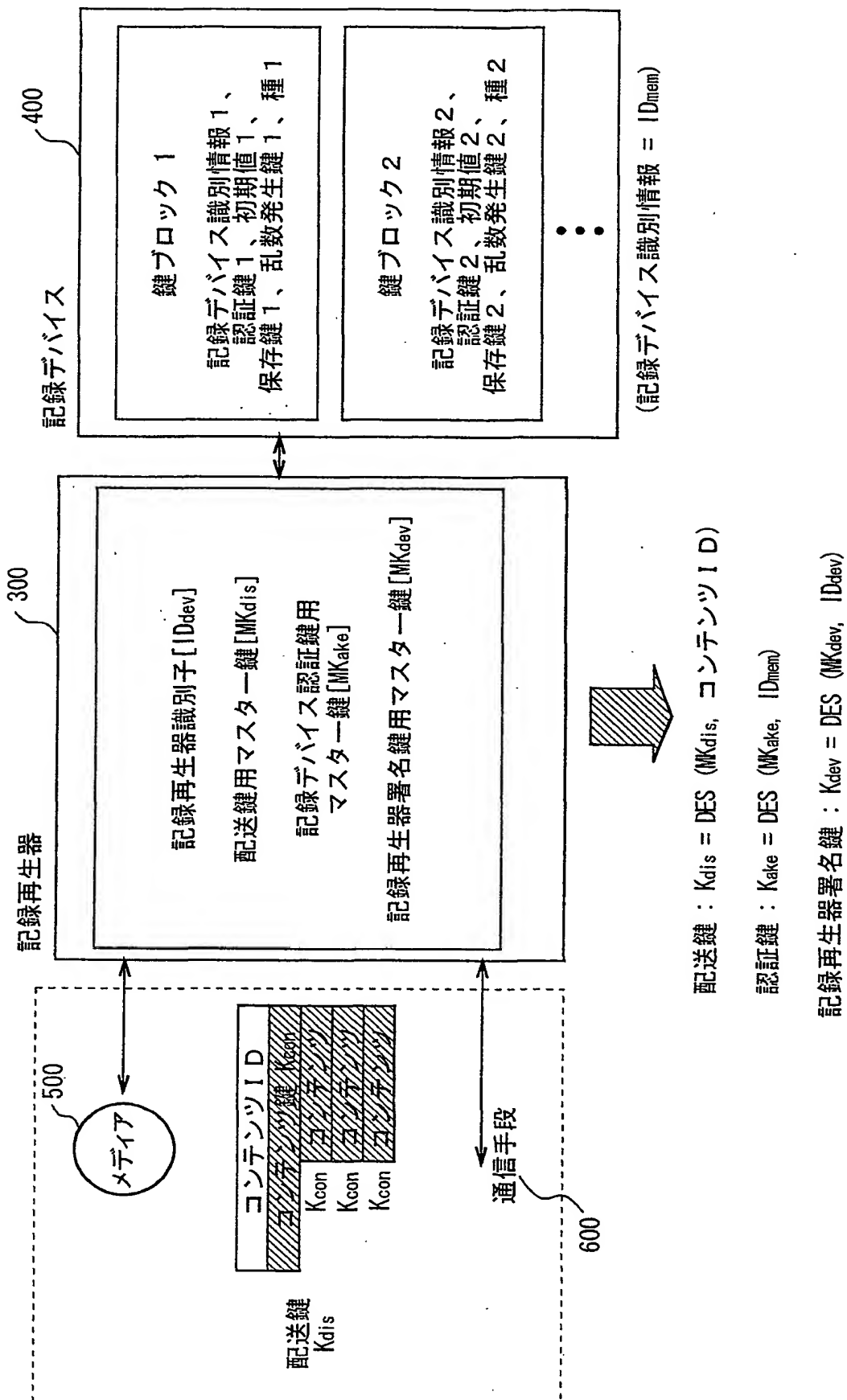
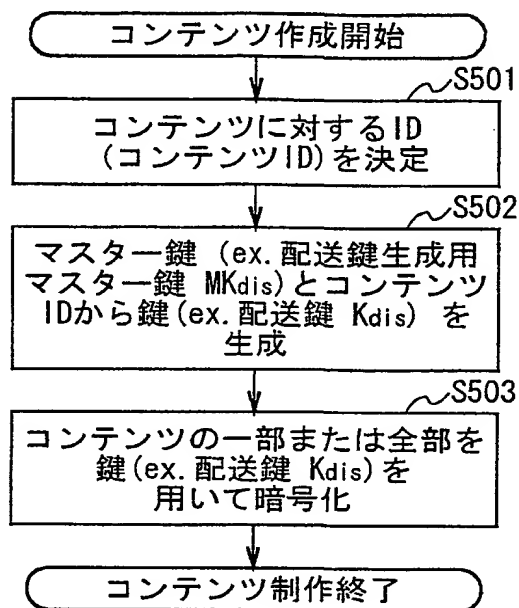


図 49

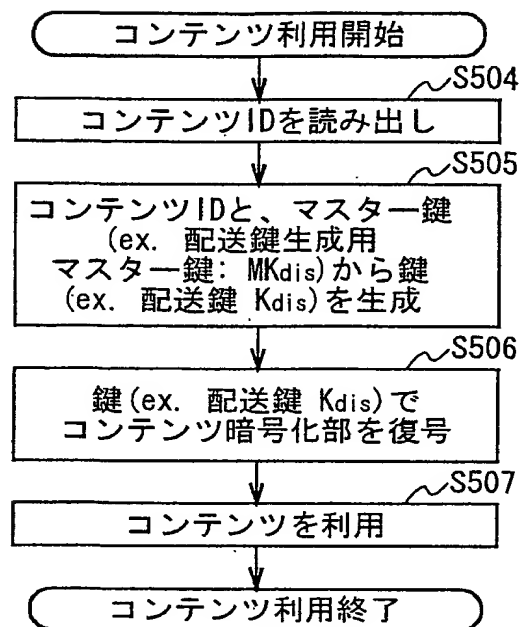
Master鍵から個別の鍵を生成する方法ー(1)

[基本フロー]

コンテンツ制作または管理者

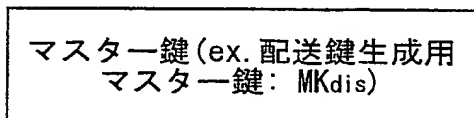


ユーザデバイス

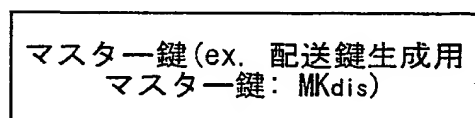


[鍵所有構成]

コンテンツ制作または管理者



ユーザデバイス



共有

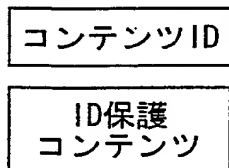
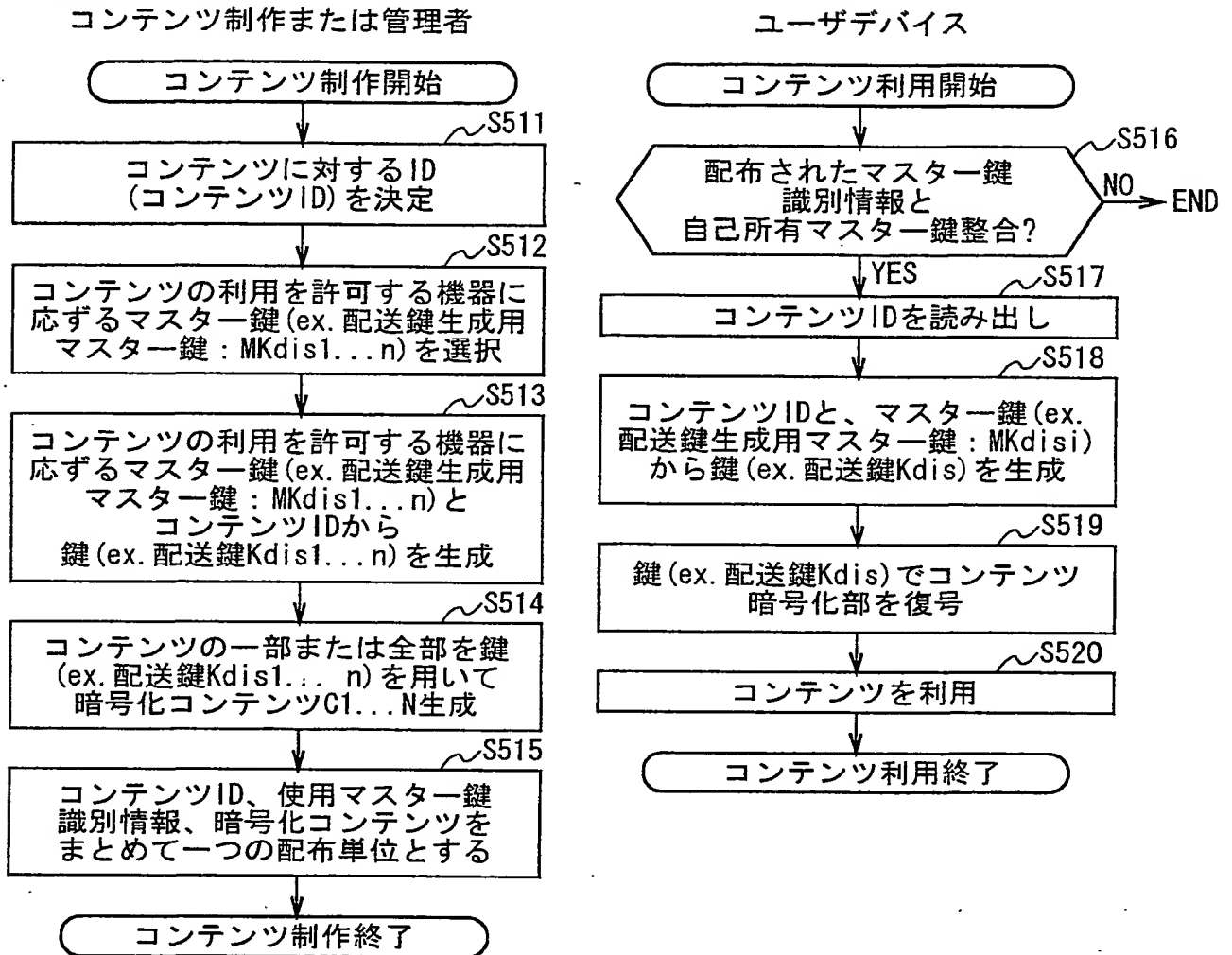


図 50

Master鍵から個別の鍵を生成する方法-(2)

[基本フロー]



[鍵所有構成]

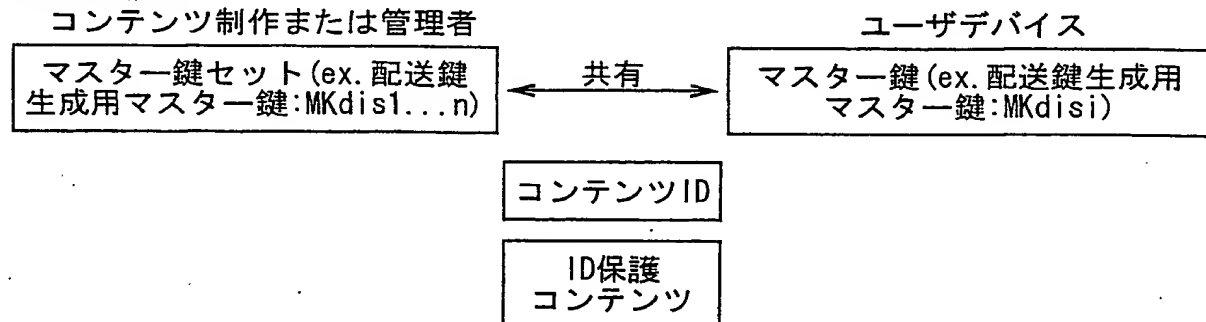


図 5 1

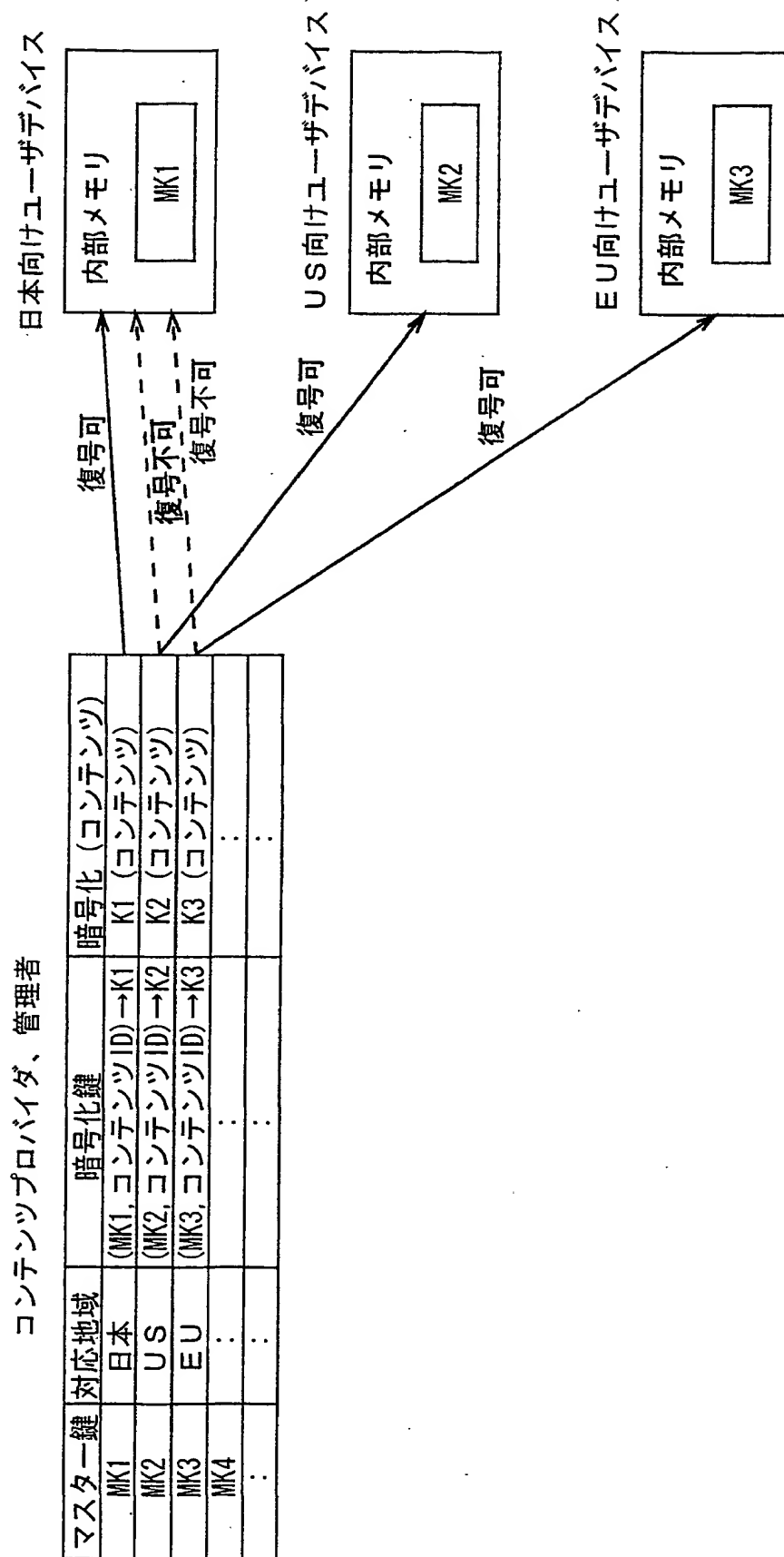
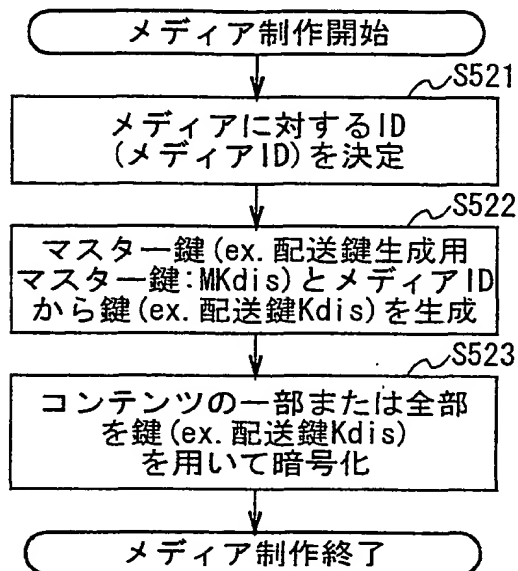


図 52

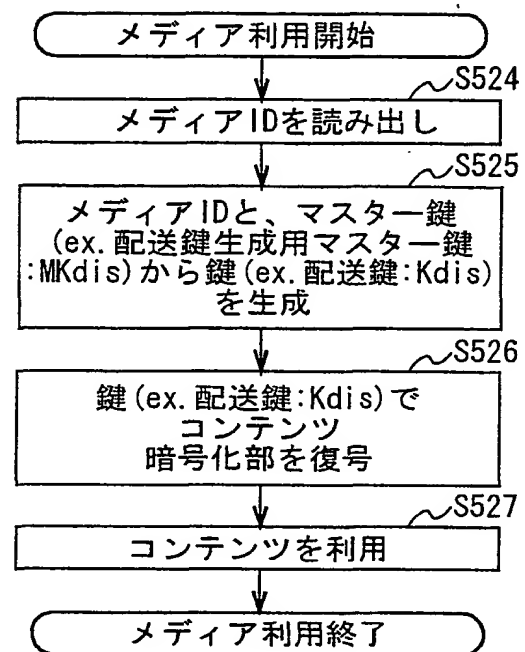
Master鍵から個別の鍵を生成する方法-(3)

[基本フロー]

メディア制作者または管理者

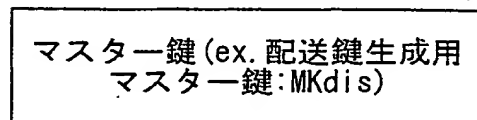


ユーザデバイス

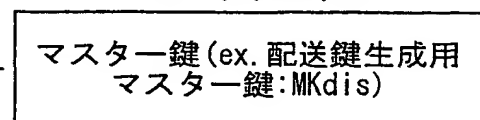


[鍵所有構成]

メディア制作者または管理者



ユーザデバイス



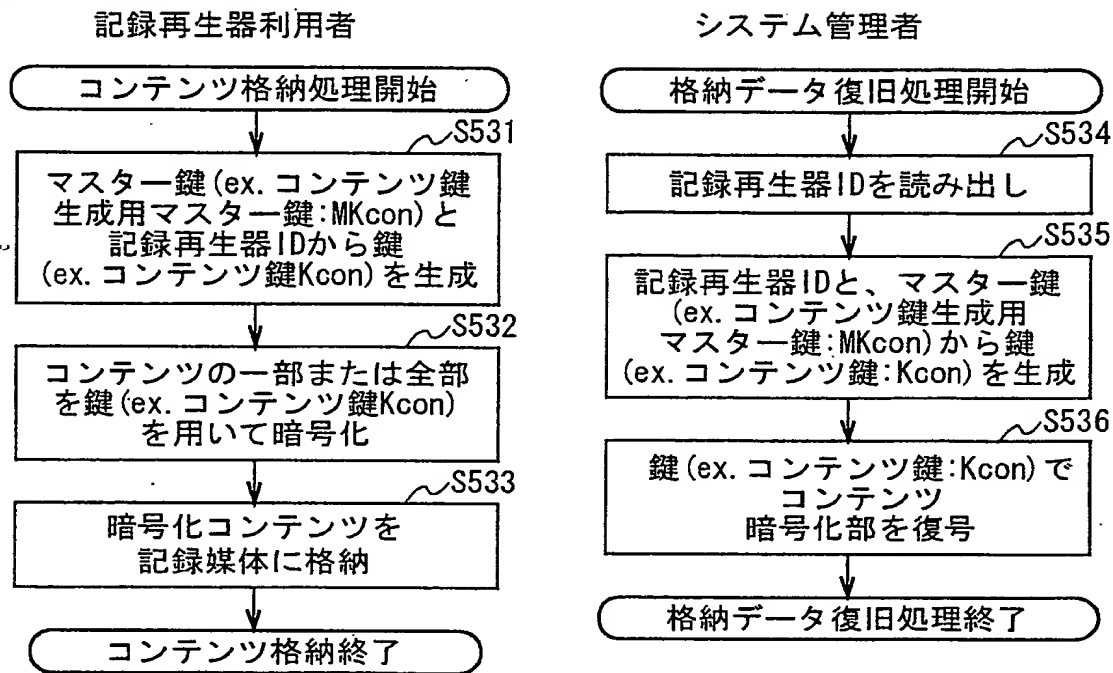
共有



図 5 3

Master鍵から個別の鍵を生成する方法－(4)

[基本フロー]



[鍵所有構成]

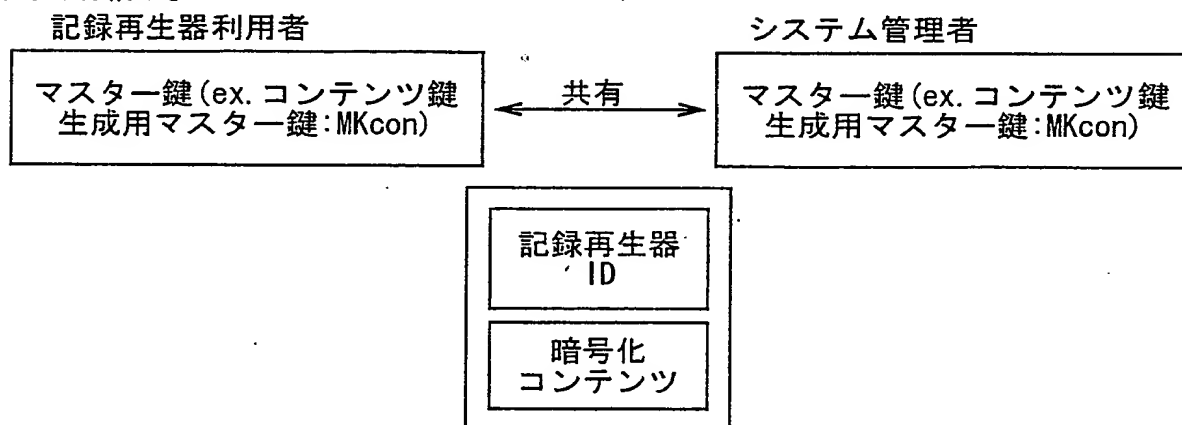
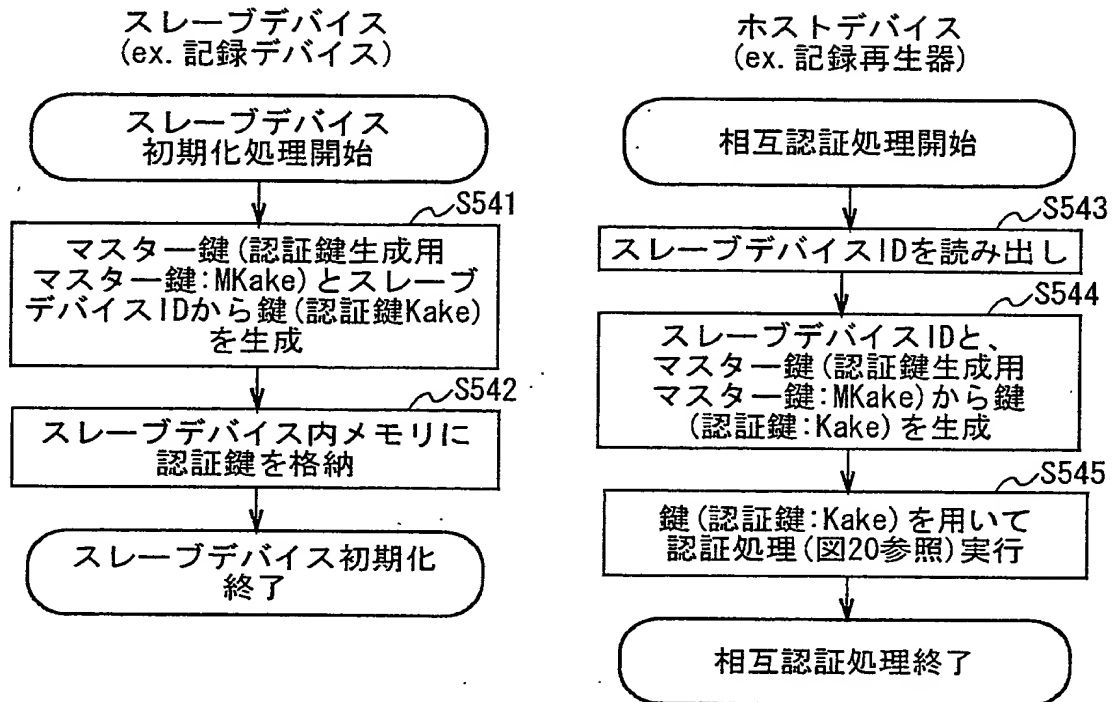


図 5 4

Master鍵から個別の鍵を生成する方法- (5)
[基本フロー]



[鍵所有構成]

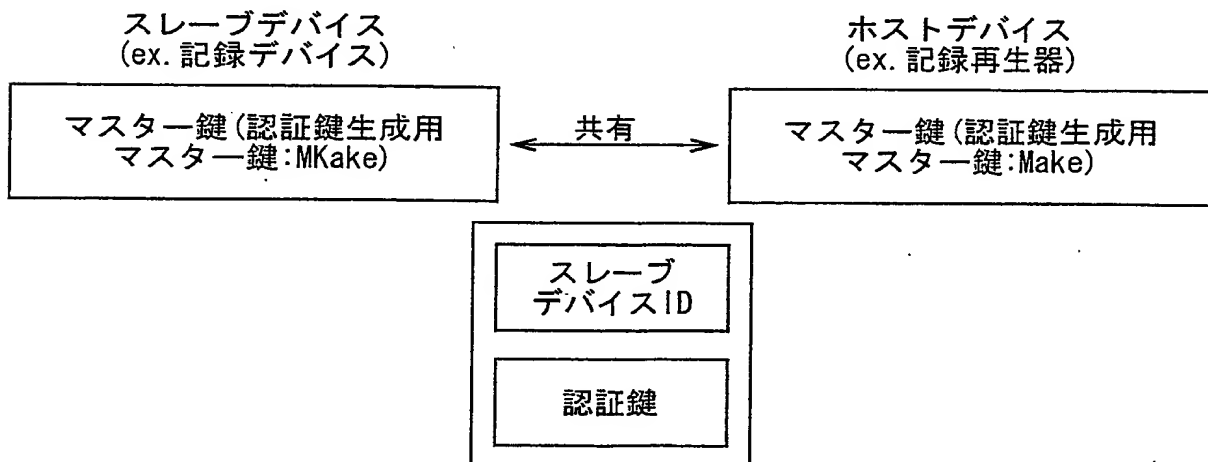
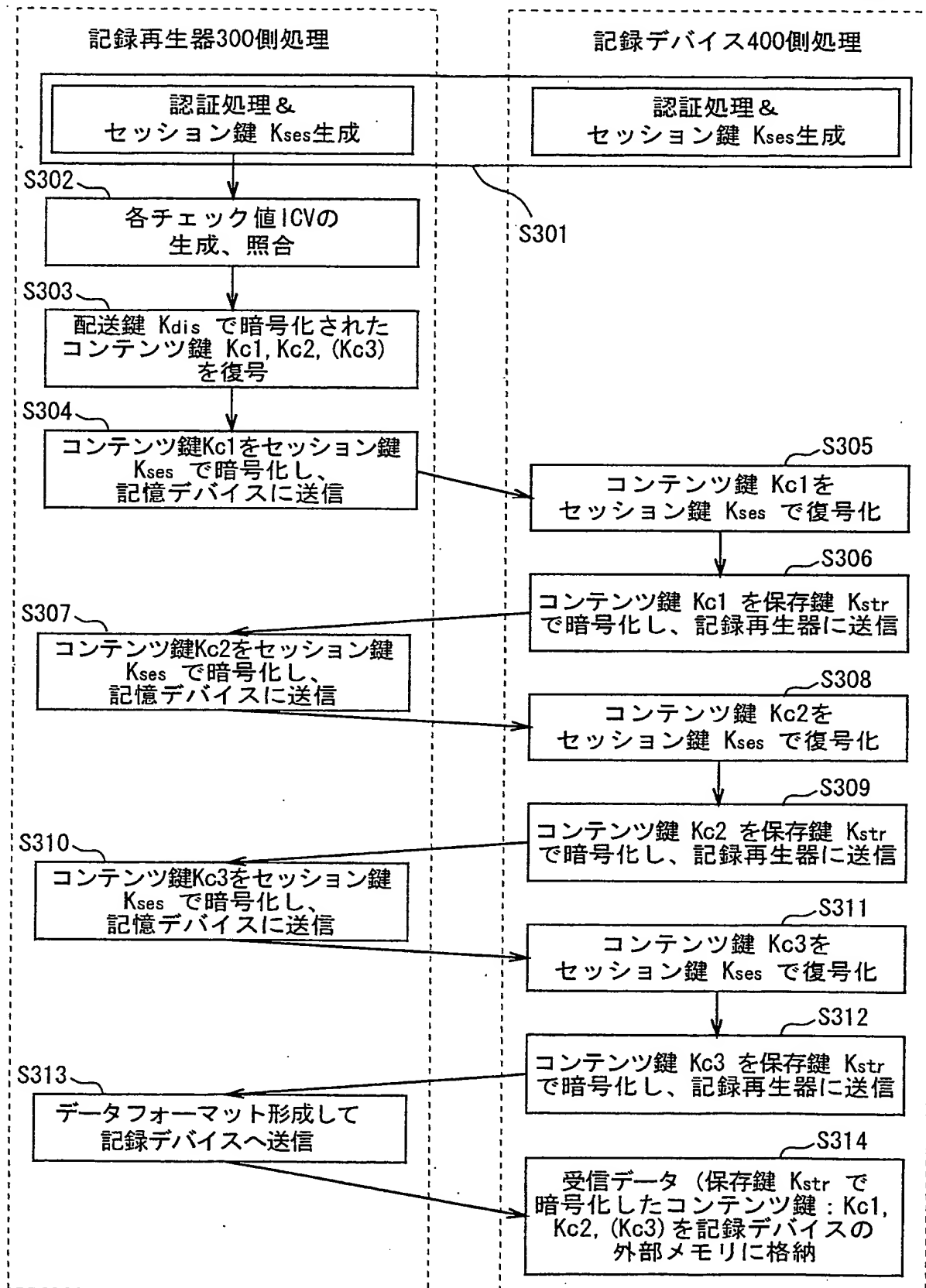


図 5 5

トリプルDESコンテンツ鍵：Kc1, Kc2, (Kc3)の格納（ダウンロード）処理



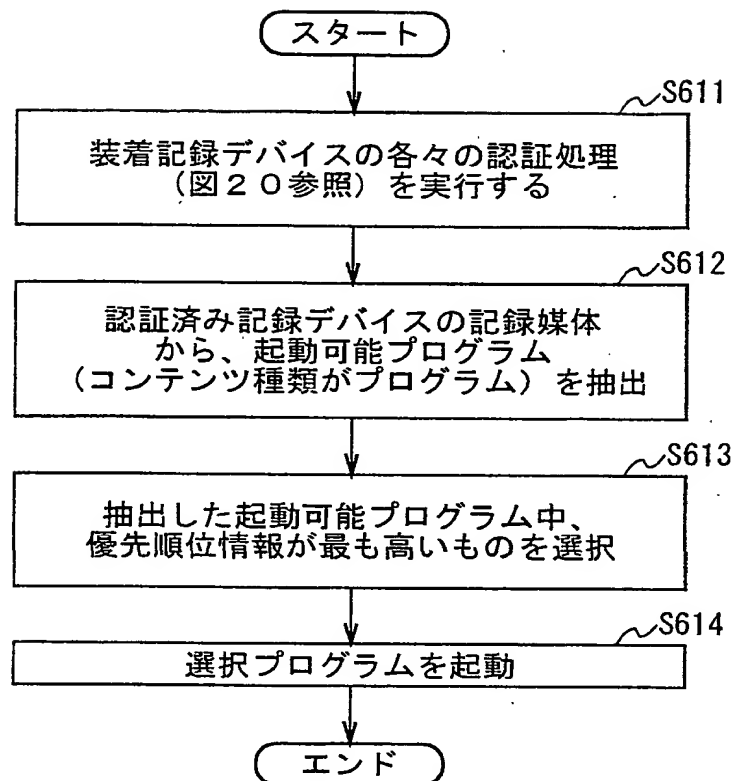


図57

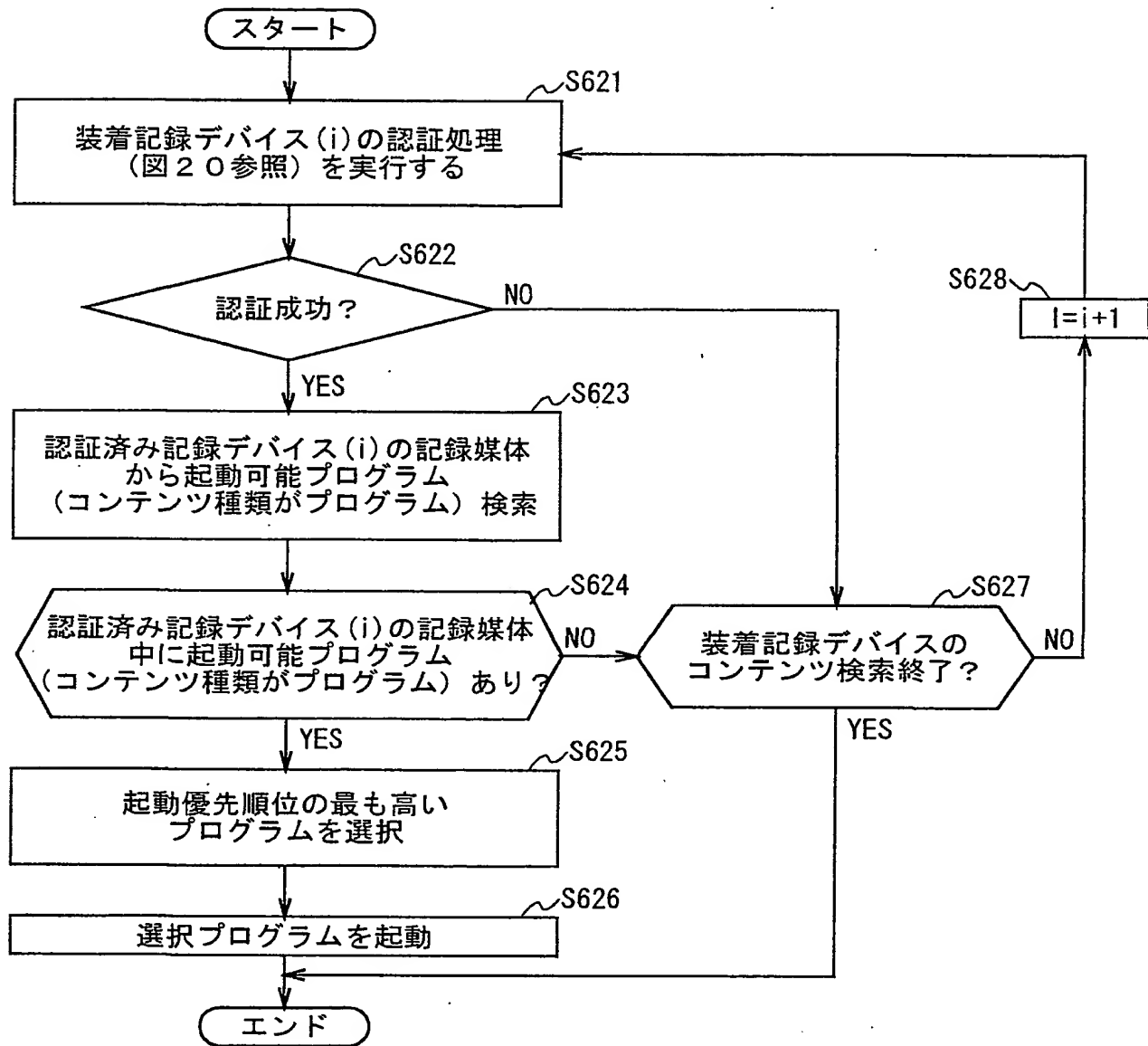


図58

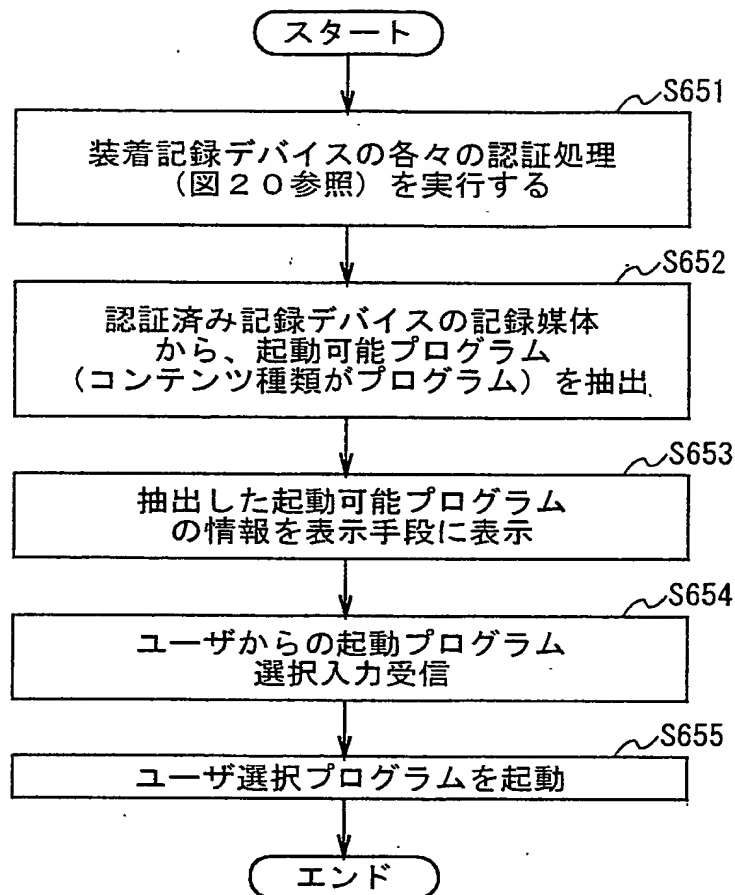


図 5 9

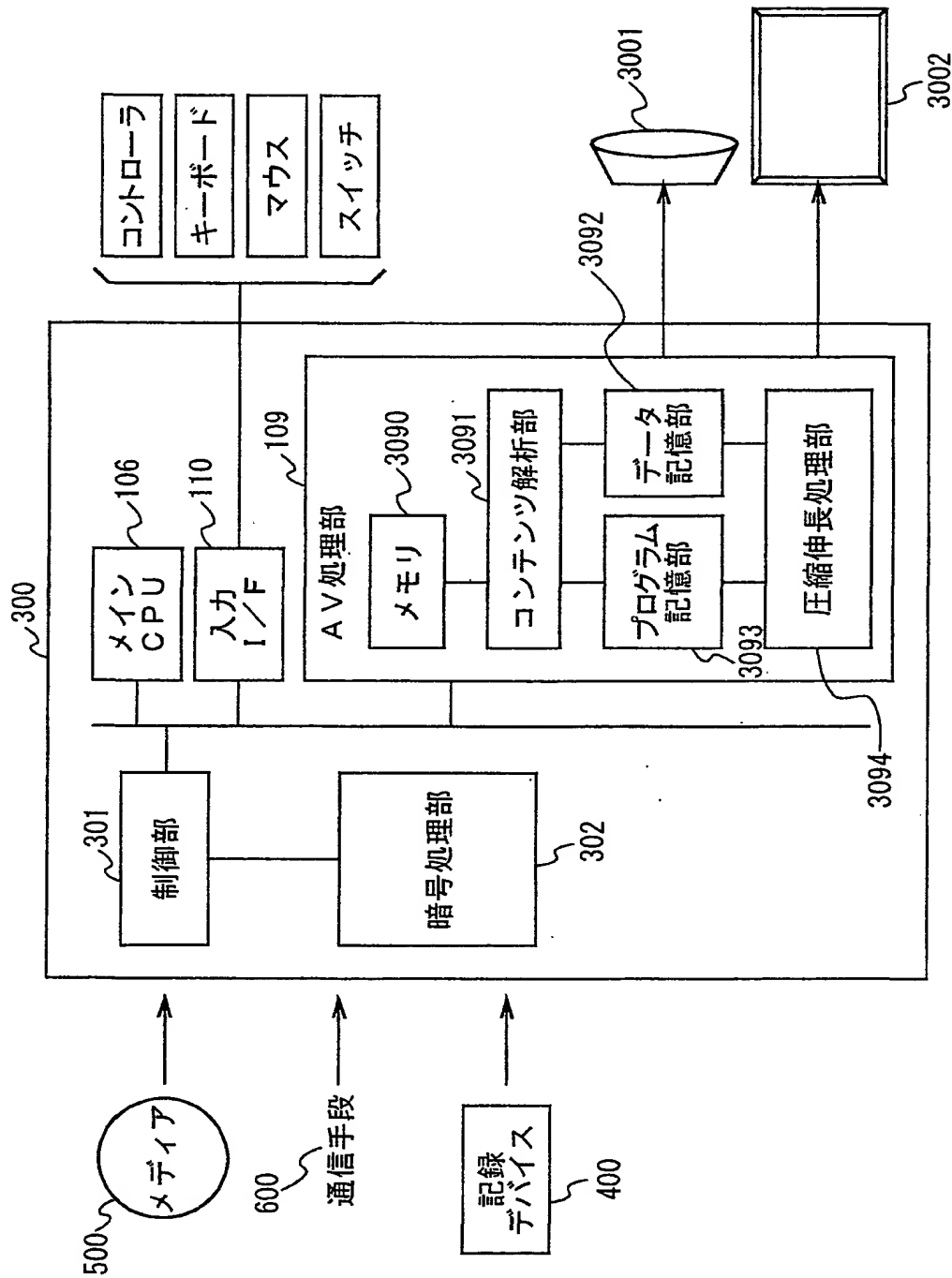


図 60

コンテンツ構成例 (1)

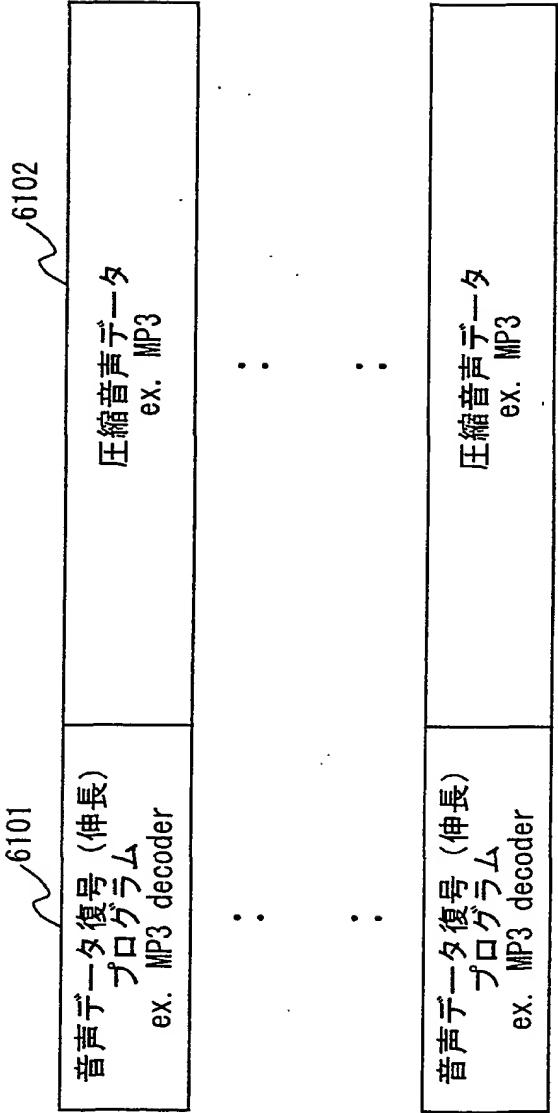


図 6 1

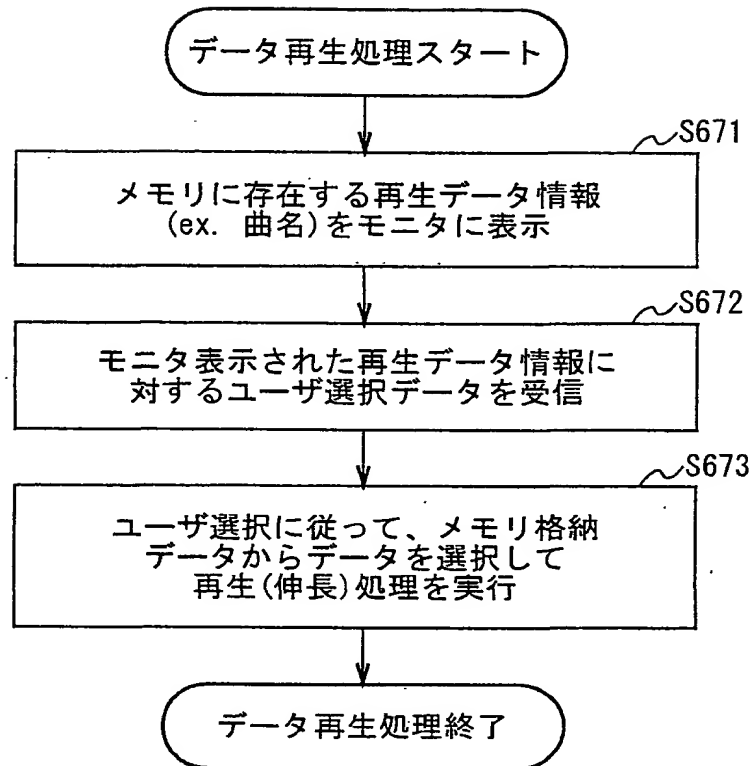


図 6 2

コンテンツ構成例 (2)

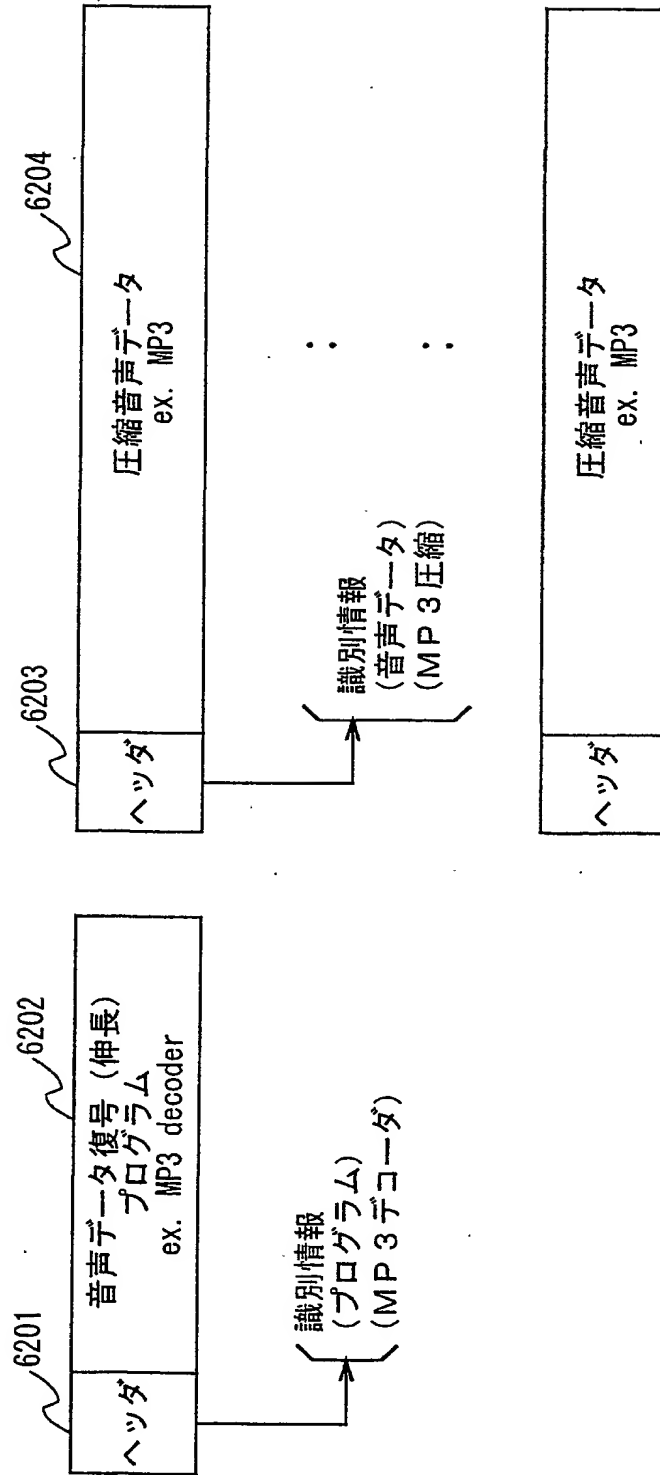


図 63

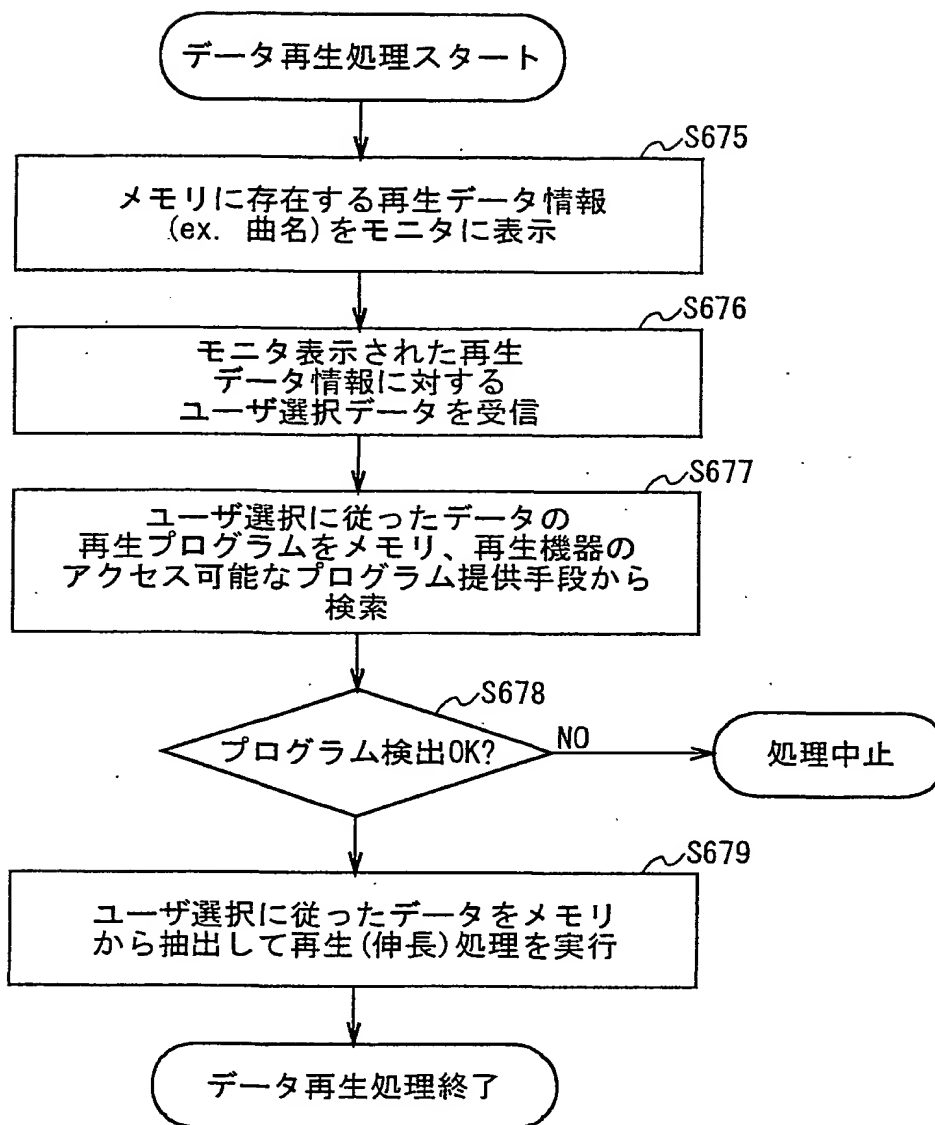


図 6 4

コンテンツ構成例 (3)

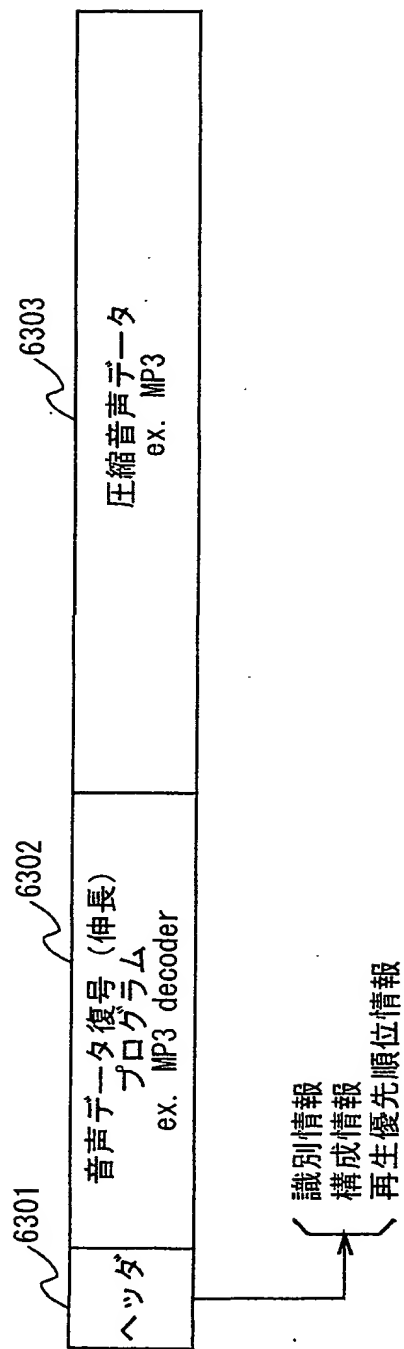


図 65

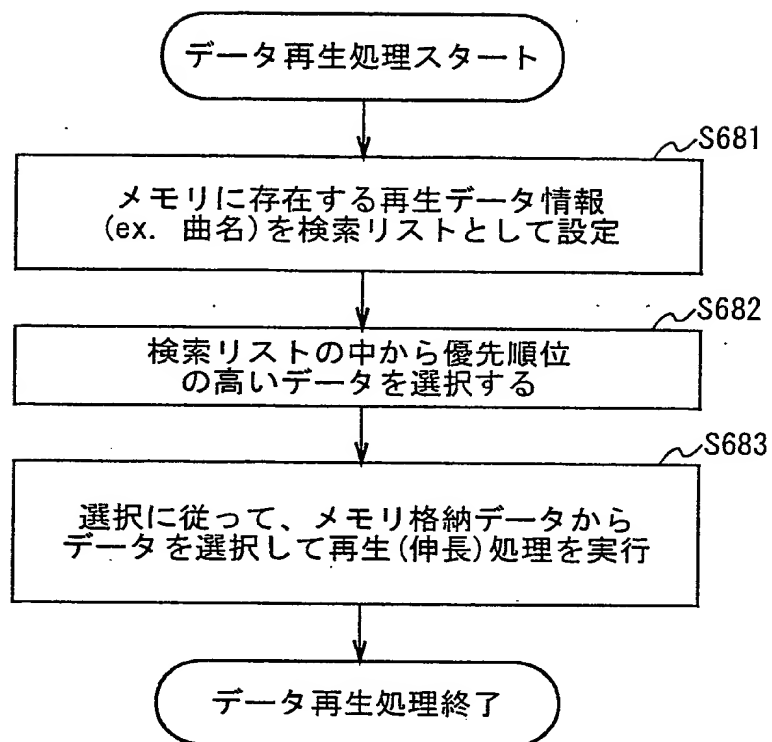


図 6 6

コンテンツ構成例 (4)

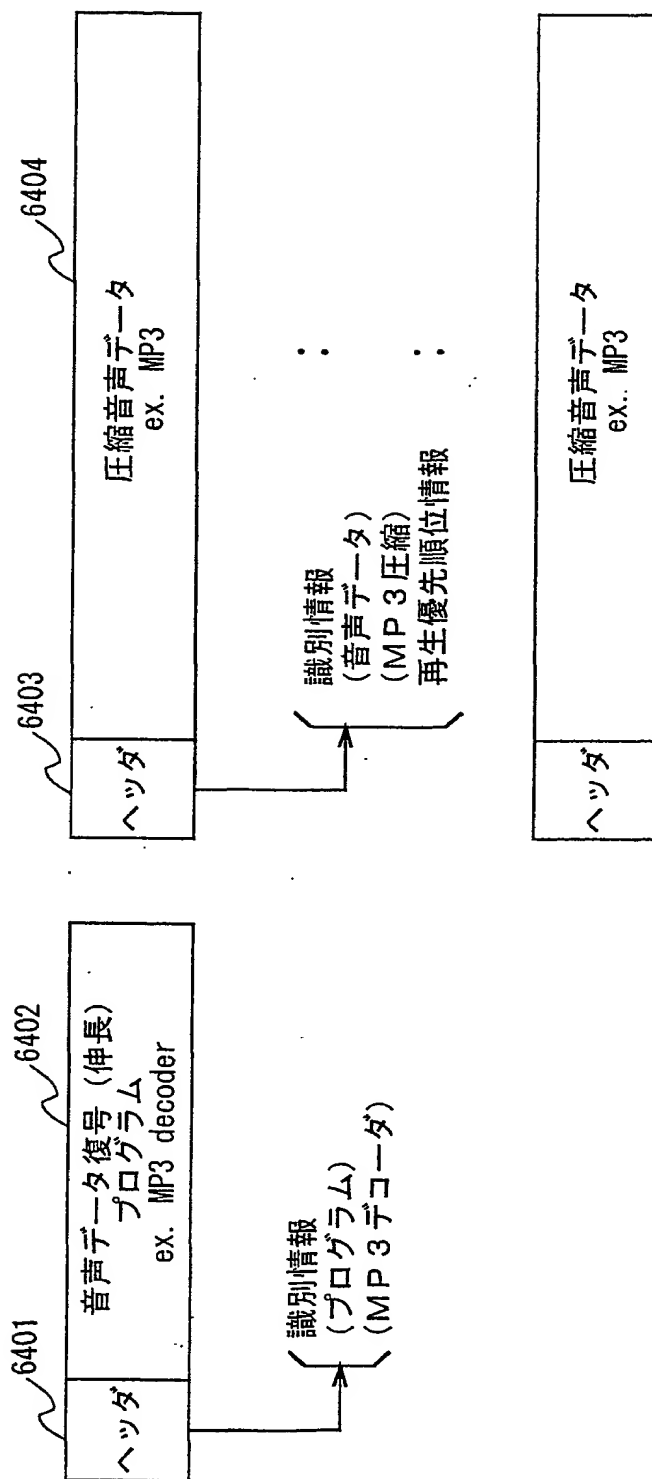


図 67

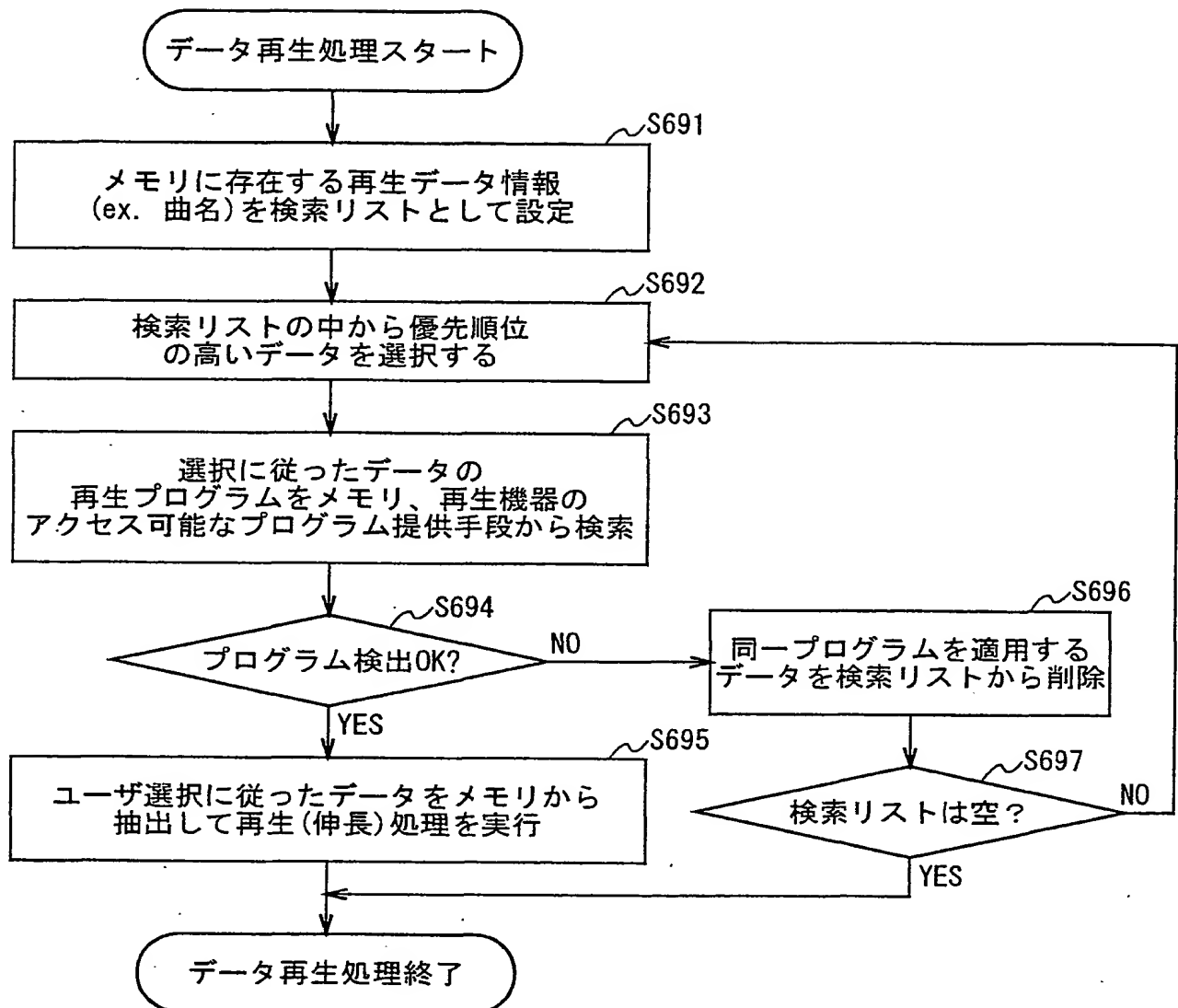
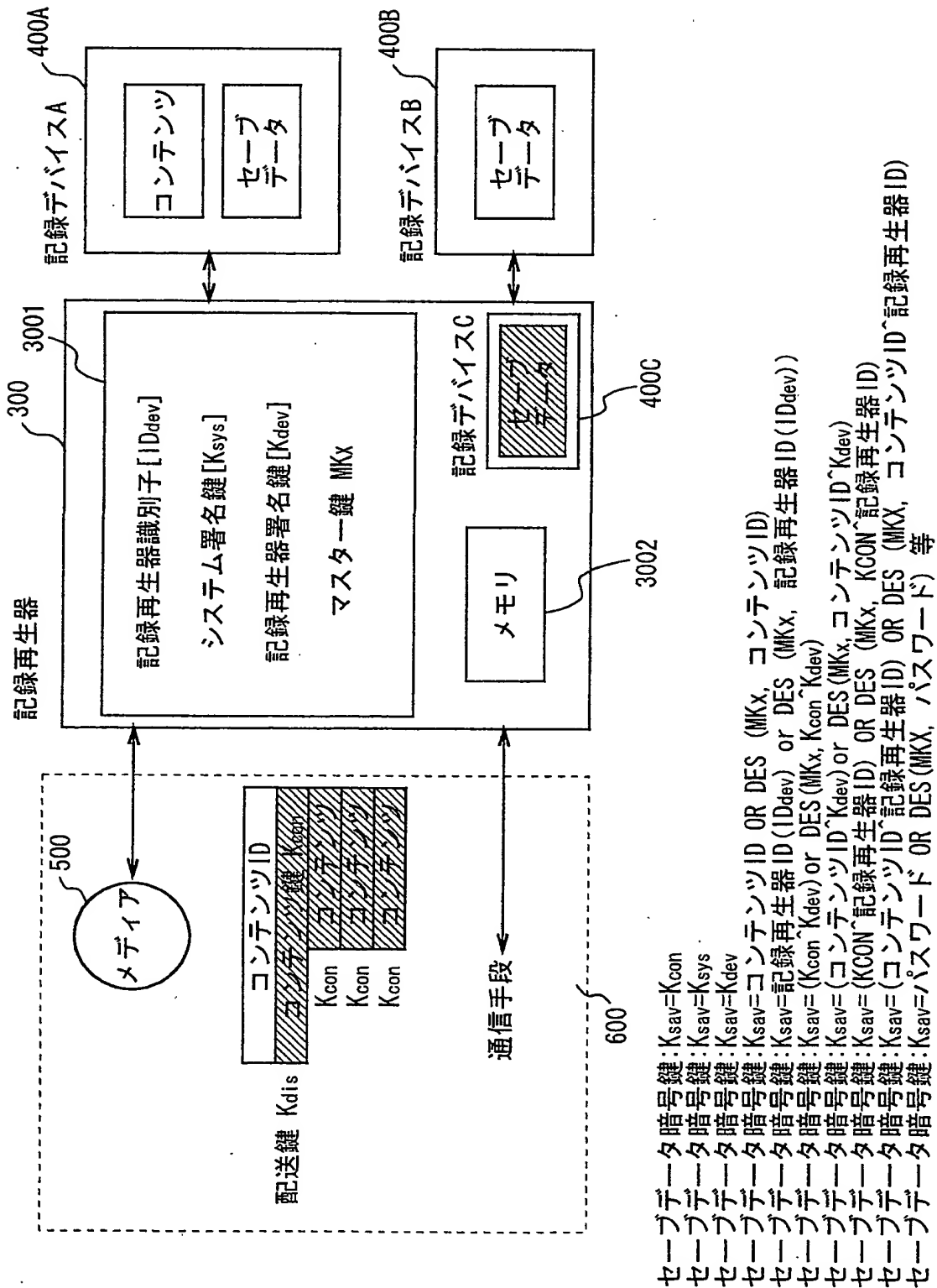


図 6 8



96 図

(1) コンテンツ固有鍵、or システム共通鍵を使用したセーブデータ格納処理例

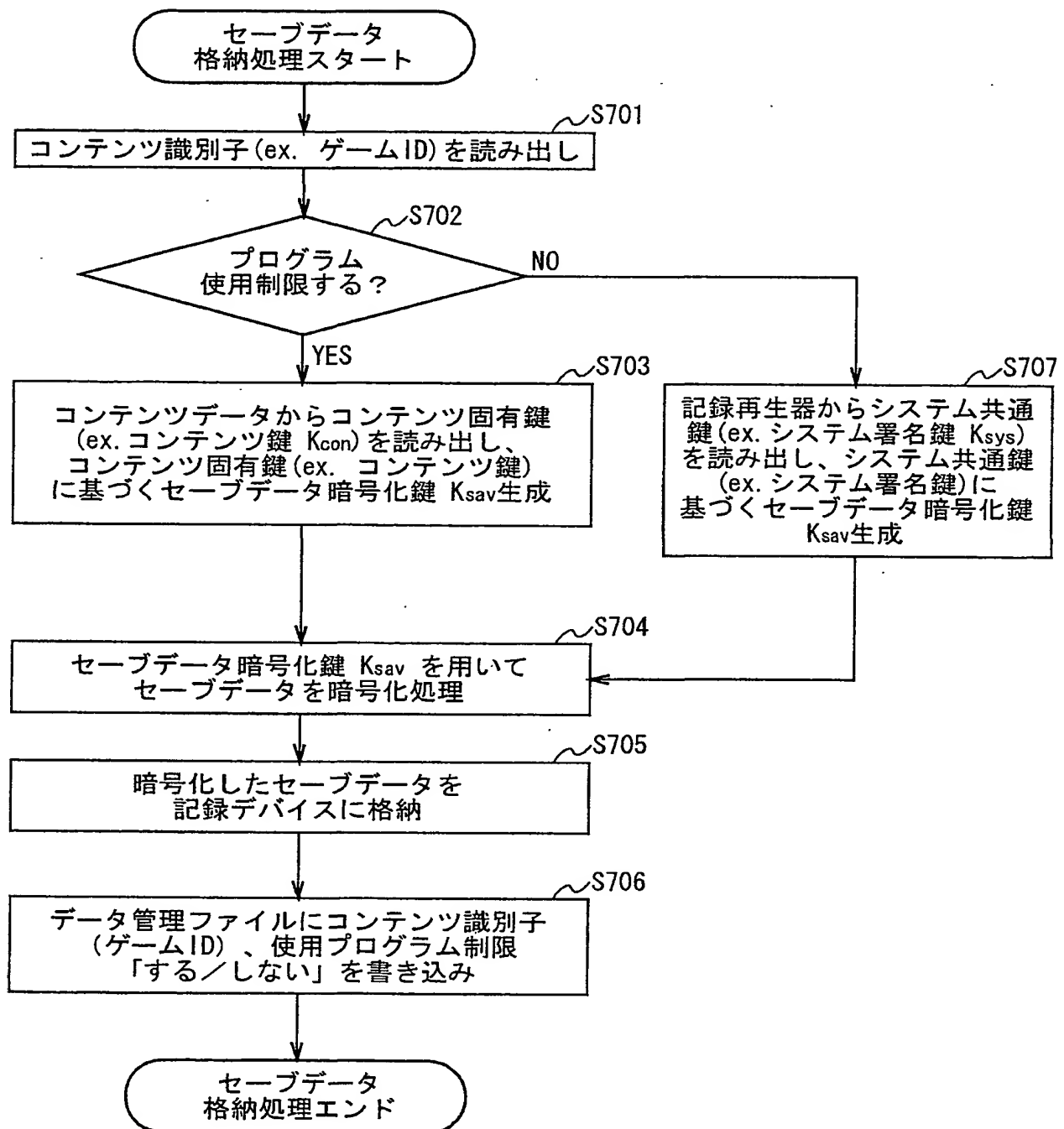


図 70

データ管理ファイル (1)

データ 番号	コンテンツ識別子 (ゲーム I D)	記録再生器識別子 (I D dev)	プログラム 使用制限
1	12345678...	56789012...	する
2	ABCDEF12...	09876543...	する
3	12245678...	58834762...	しない
⋮	⋮	⋮	⋮

図 7 1

(2) コンテンツ固有鍵、or システム共通鍵を使用したセーブデータ再生処理例

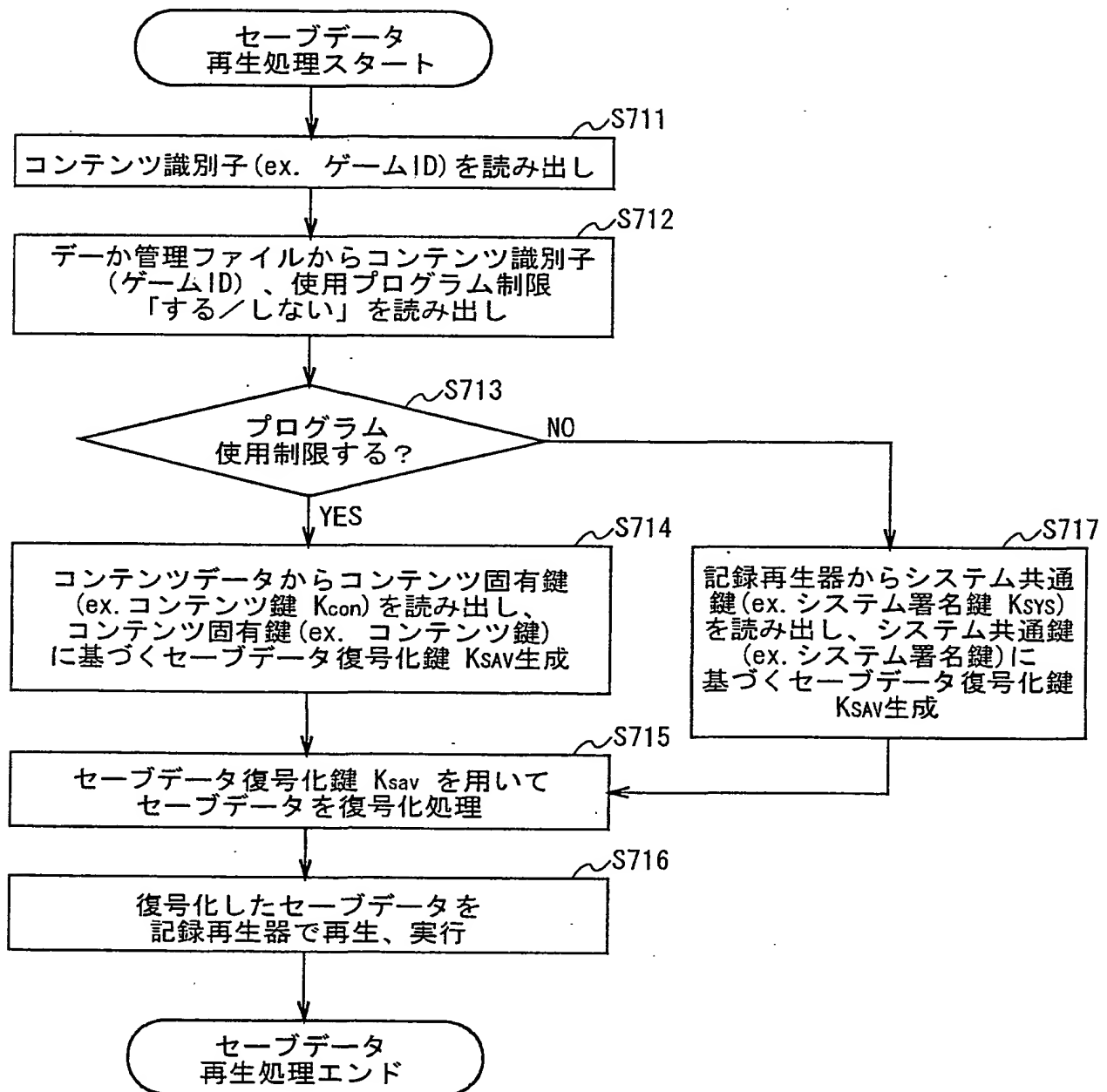


図 7 2

(3) コンテンツID、or システム共通鍵を使用したセーブデータ格納処理例

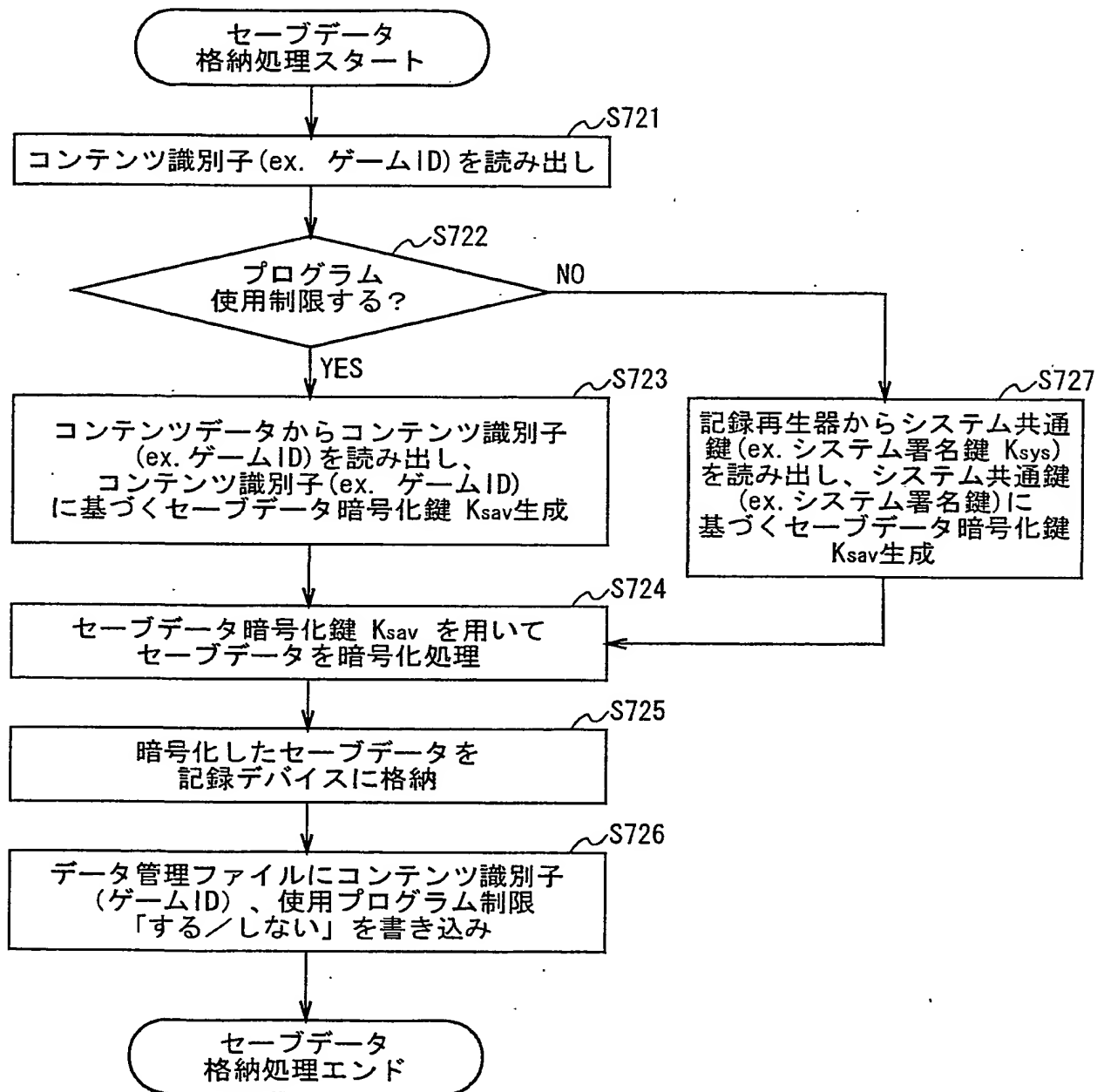


図 7 3

(4) コンテンツID、or システム共通鍵を使用したセーブデータ再生処理例

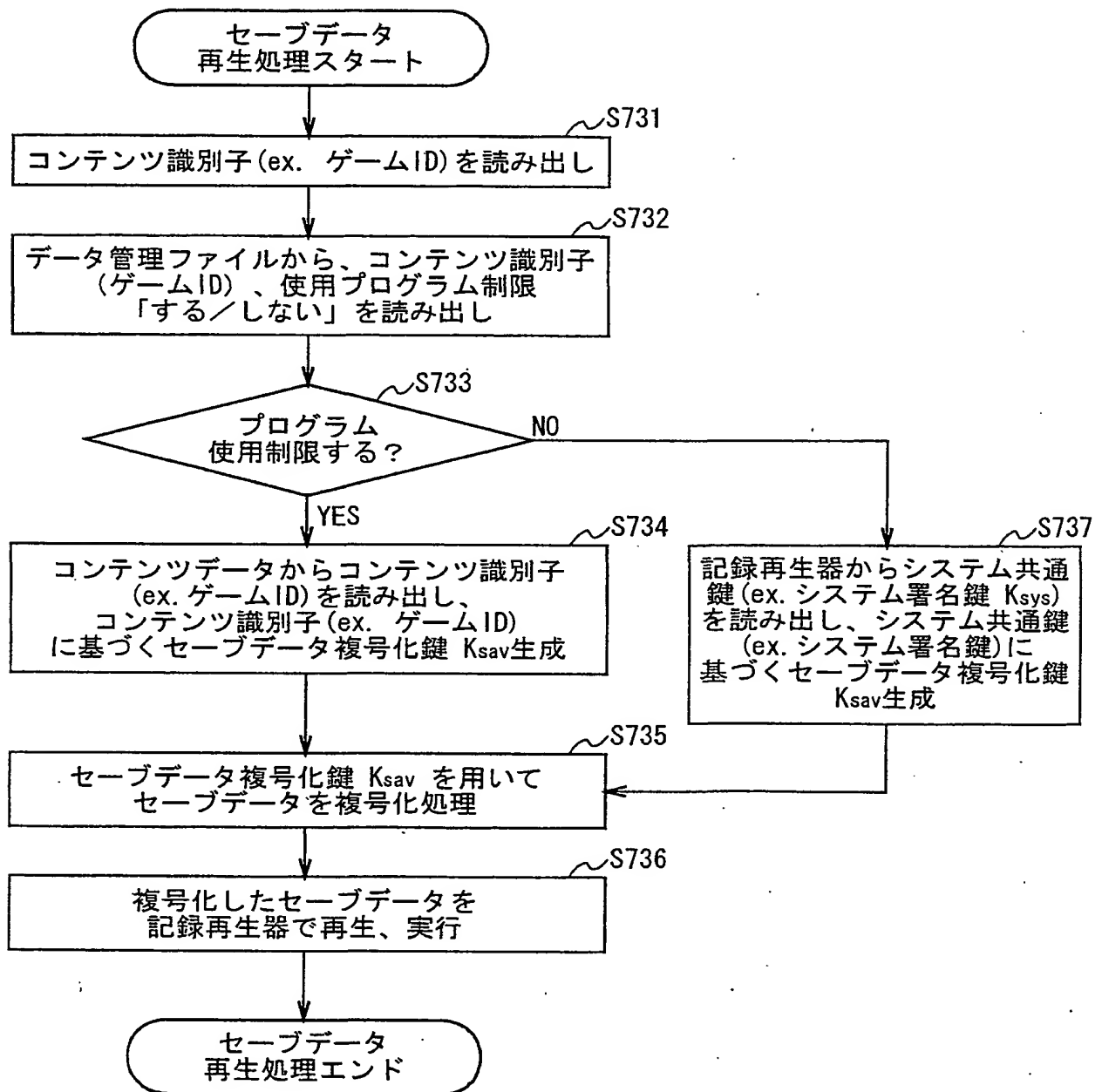


図 7 4

(5) 記録再生器固有鍵、or システム共通鍵を使用したセーブデータ格納処理例

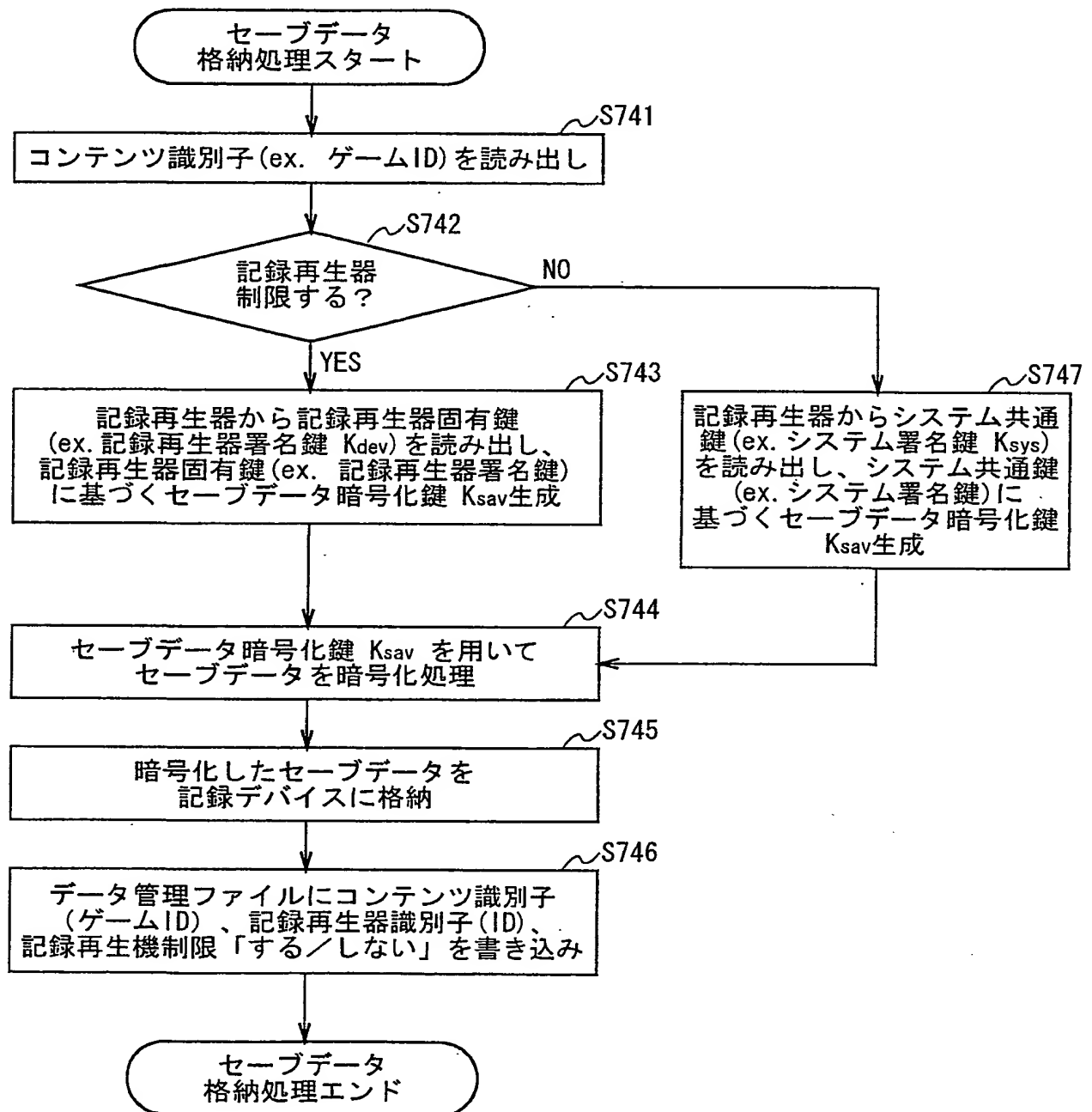


図 7 5

データ管理ファイル (2)

データ 番号	コンテンツ識別子 (ゲームID)	記録再生器識別子 (ID dev)	記録再生器 制限
1	12345678...	56789012...	しない
2	ABCDEF12...	09876543...	する
3	12245678...	58834762...	する
⋮	⋮	⋮	⋮

図 76

(6) 記録再生器固有鍵、or システム共通鍵を使用したセーブデータ再生処理例

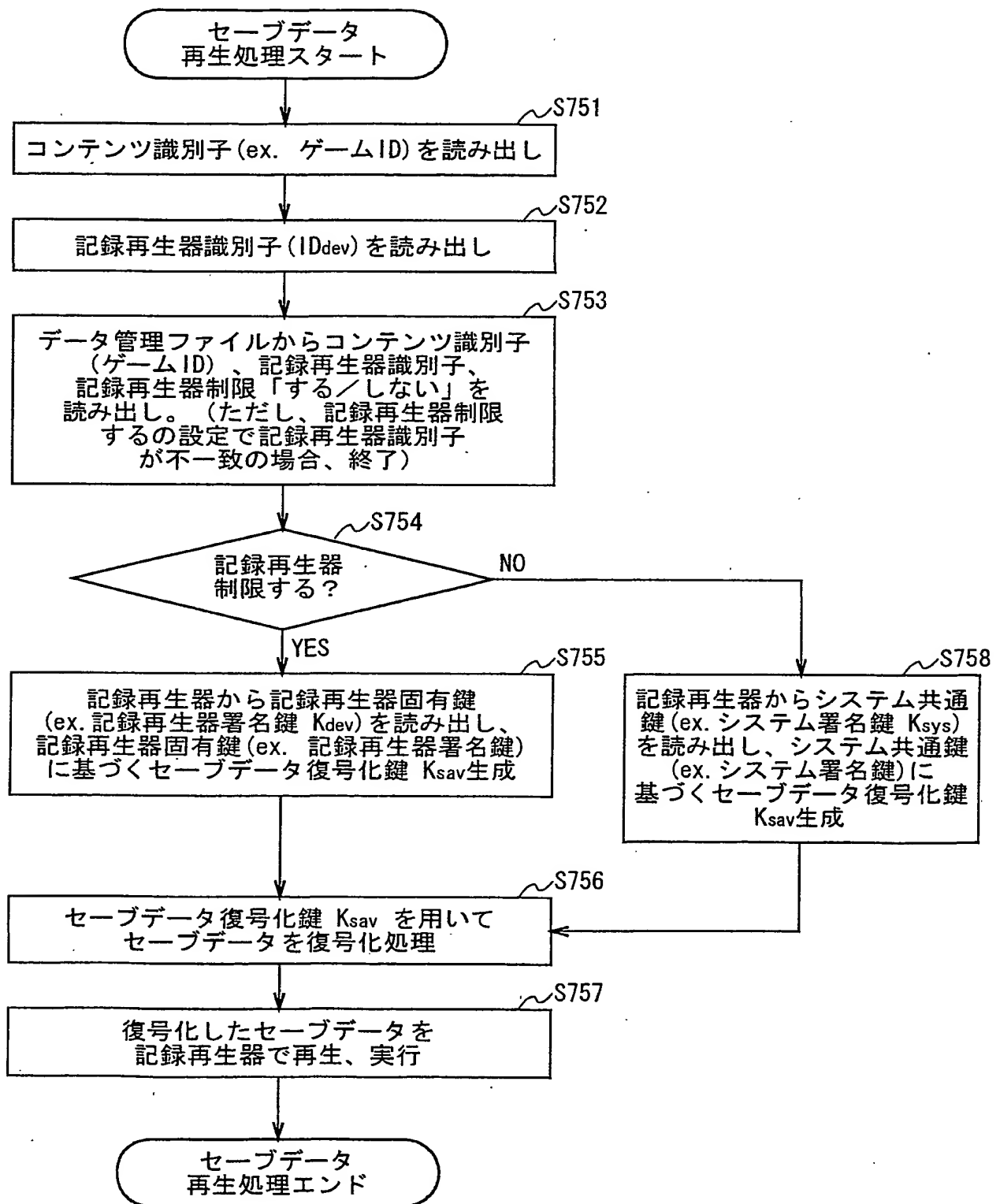


図 7 7

(7) 記録再生器識別子、or システム共通鍵を使用したセーブデータ格納処理例

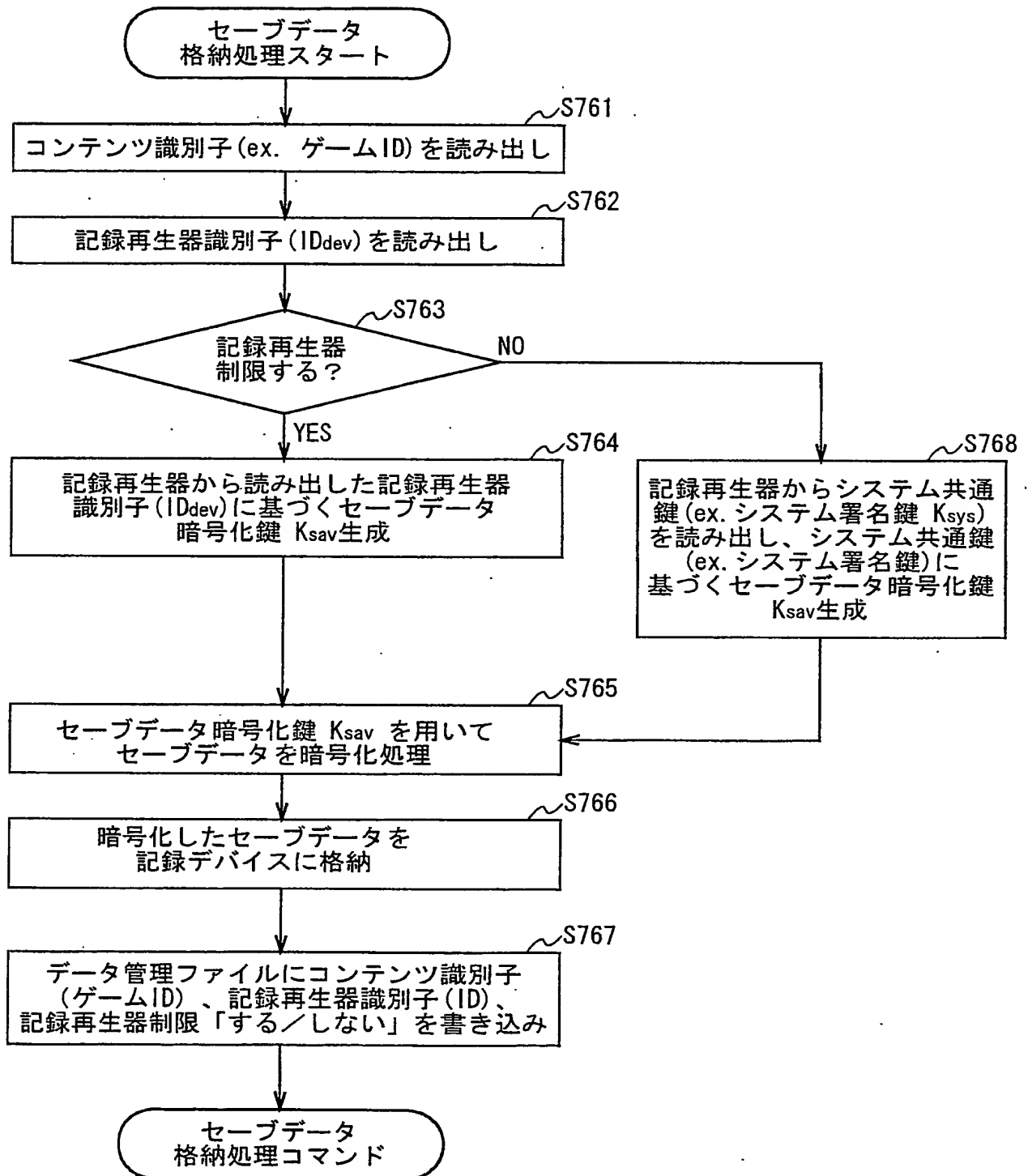
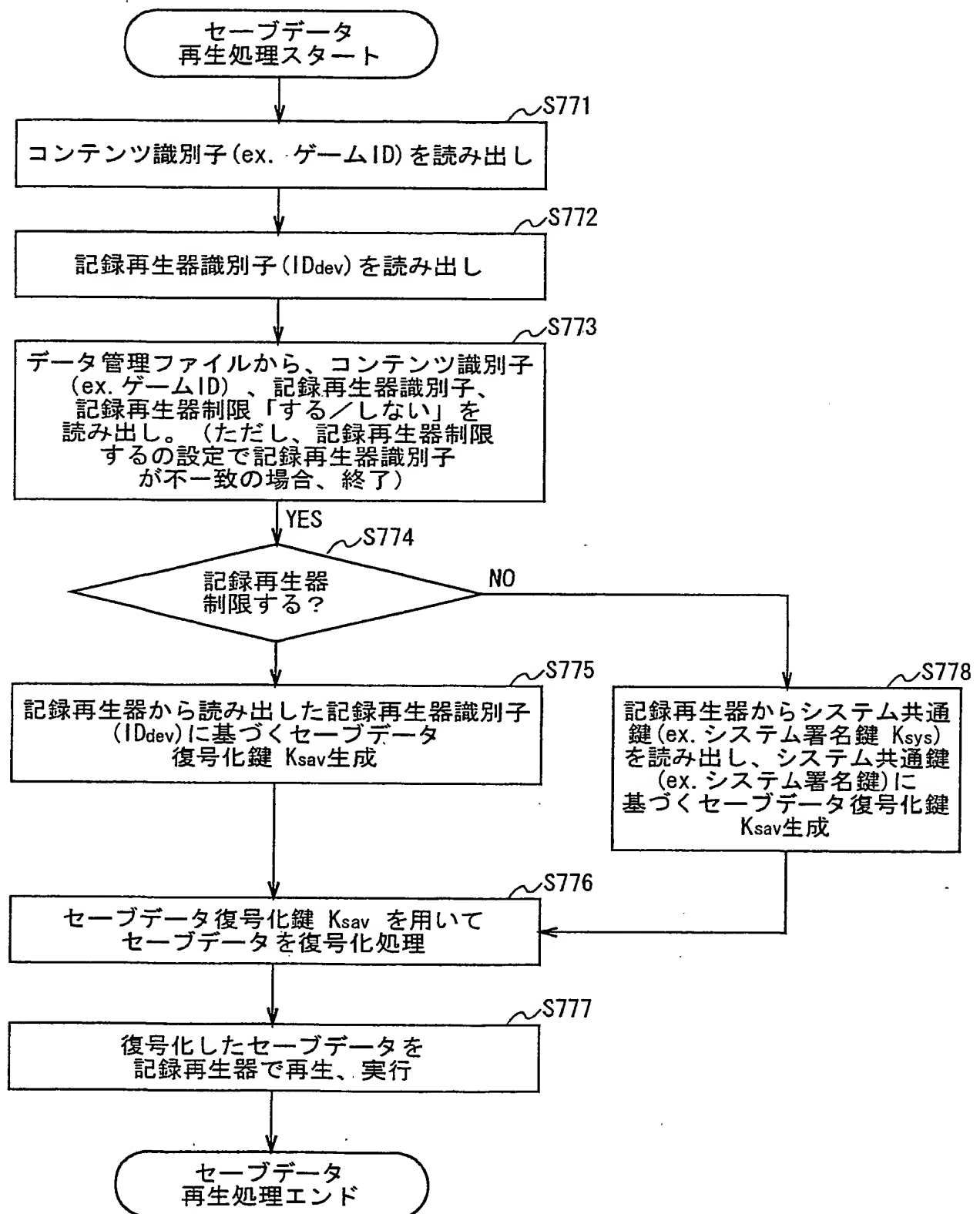


図 7 8

(8) 記録再生器識別子、or システム共通鍵を使用したセーブデータ再生処理例



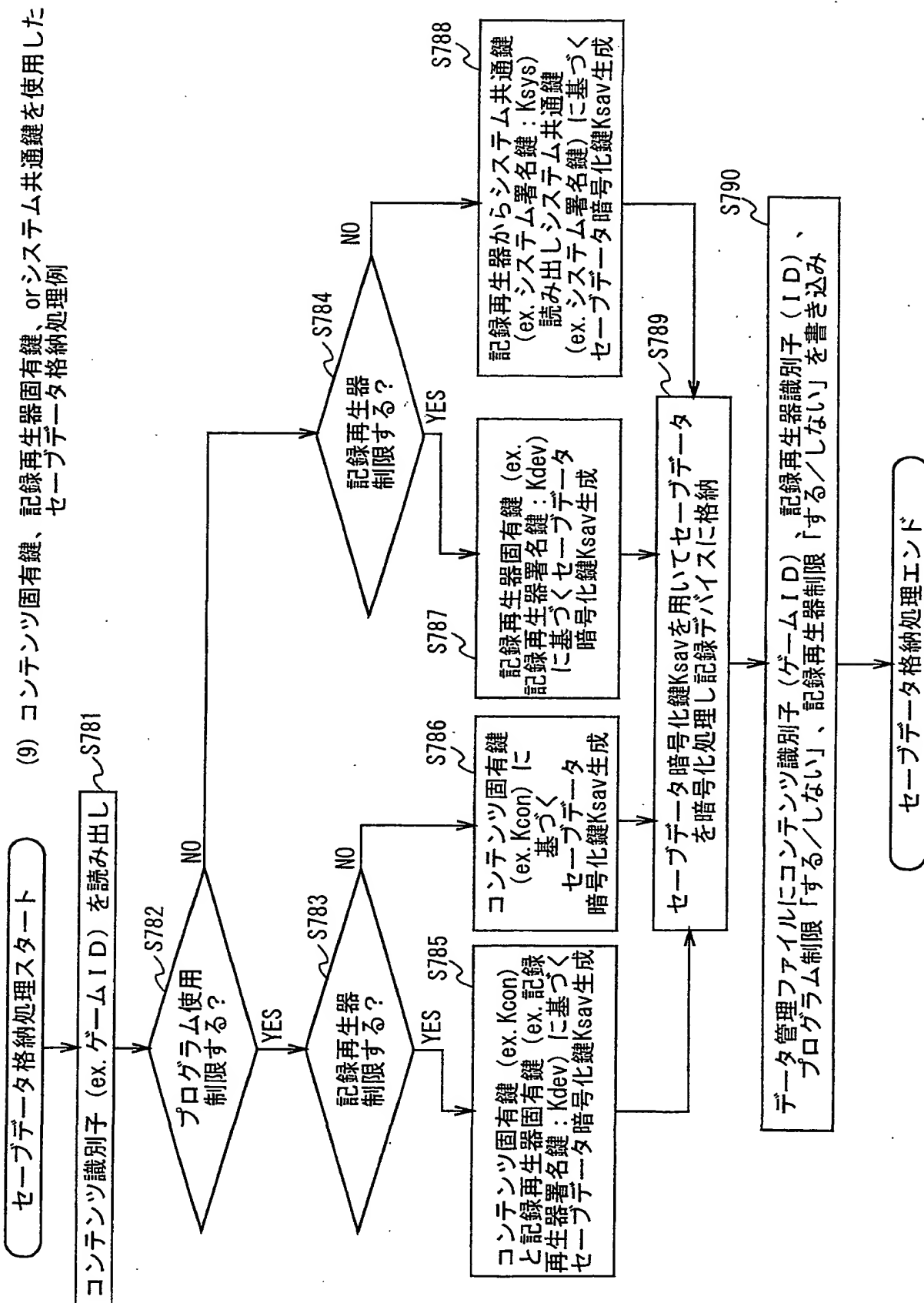


図 80

データ管理ファイル (3)

データ 番号	コンテンツ識別子 (ゲームID)	記録再生器識別子 (ID dev)	プログラム 使用制限	記録再生器 制限
1	12345678...	56789012...	する	しない
2	ABCDEF12...	09876543...	する	する
3	12245678...	58834762...	しない	する
⋮	⋮	⋮	⋮	⋮

図 8 1

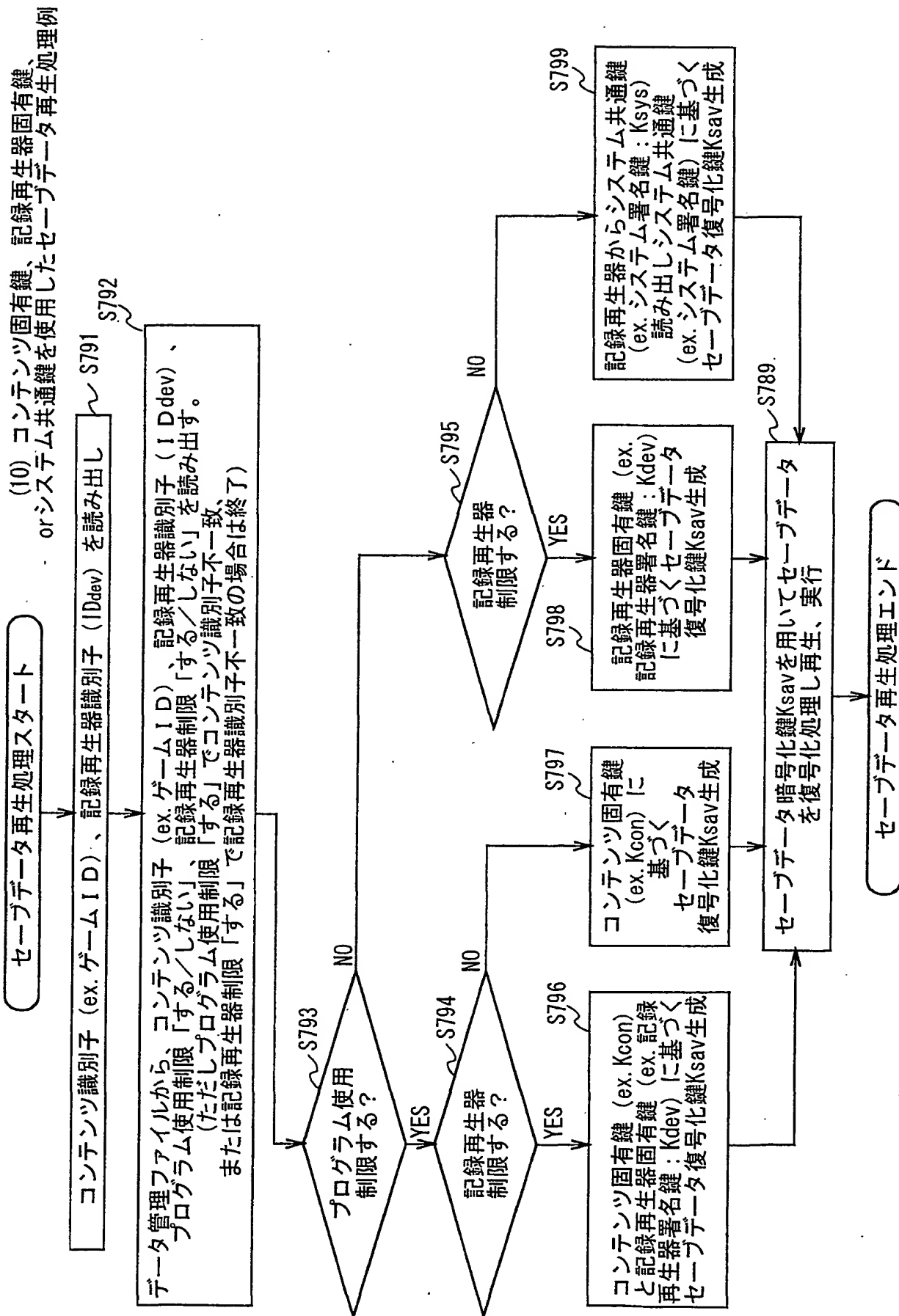


図 8 2

(11) ユーザパスワード、or システム共通鍵を使用したセーブデータ格納処理例

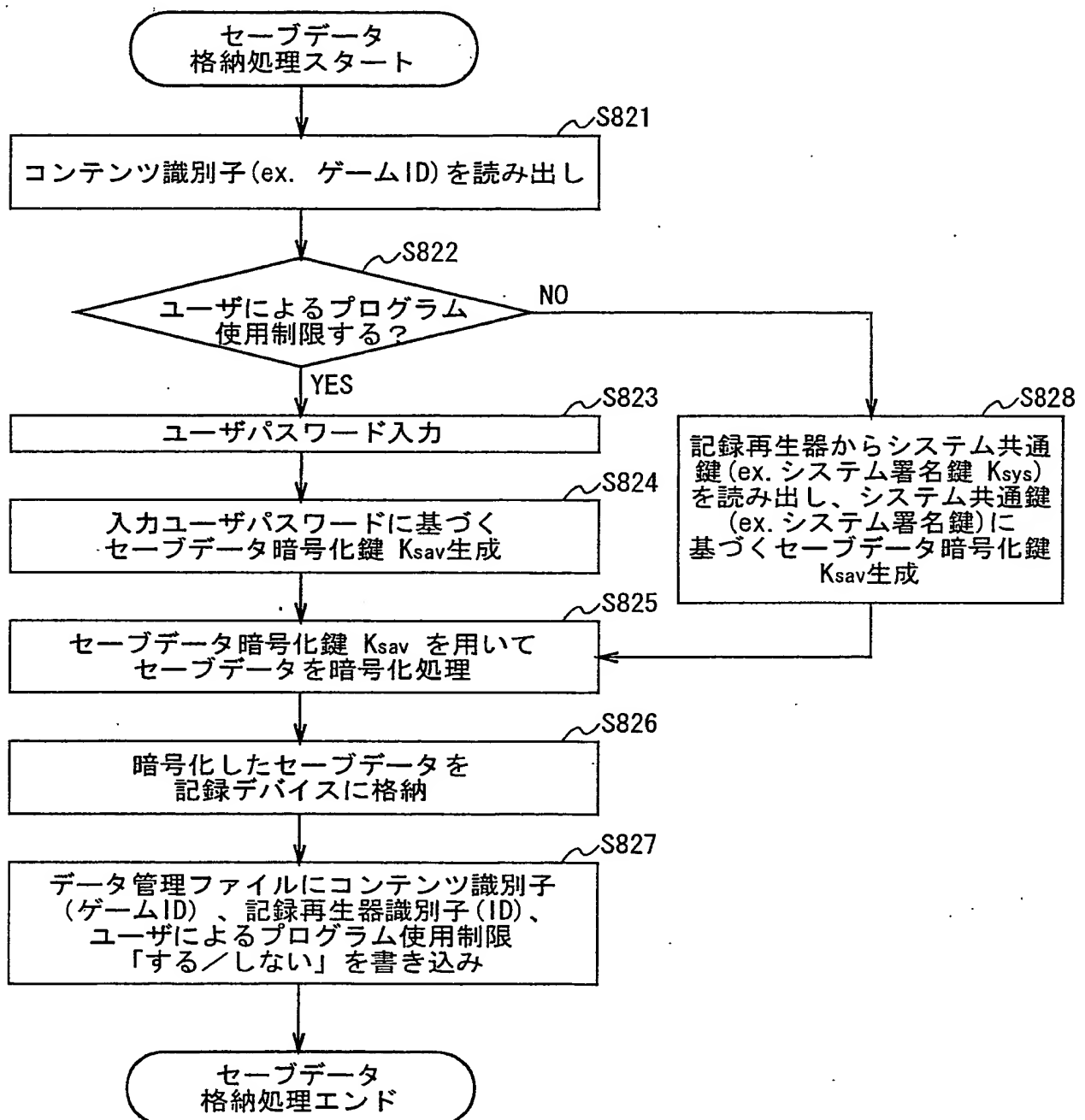


図 8 3

データ管理ファイル (4)

データ 番号	コンテンツ識別子 (ゲームID)	記録再生器識別子 (ID dev)	ユーザによる プログラム使用制限
1	12345678...	56789012...	する
2	ABCDEF12...	09876543...	する
3	12245678...	58834762...	しない
:	:	:	:

図 8 4

(12) ユーザパスワード、or システム共通鍵を使用したセーブデータ再生処理例

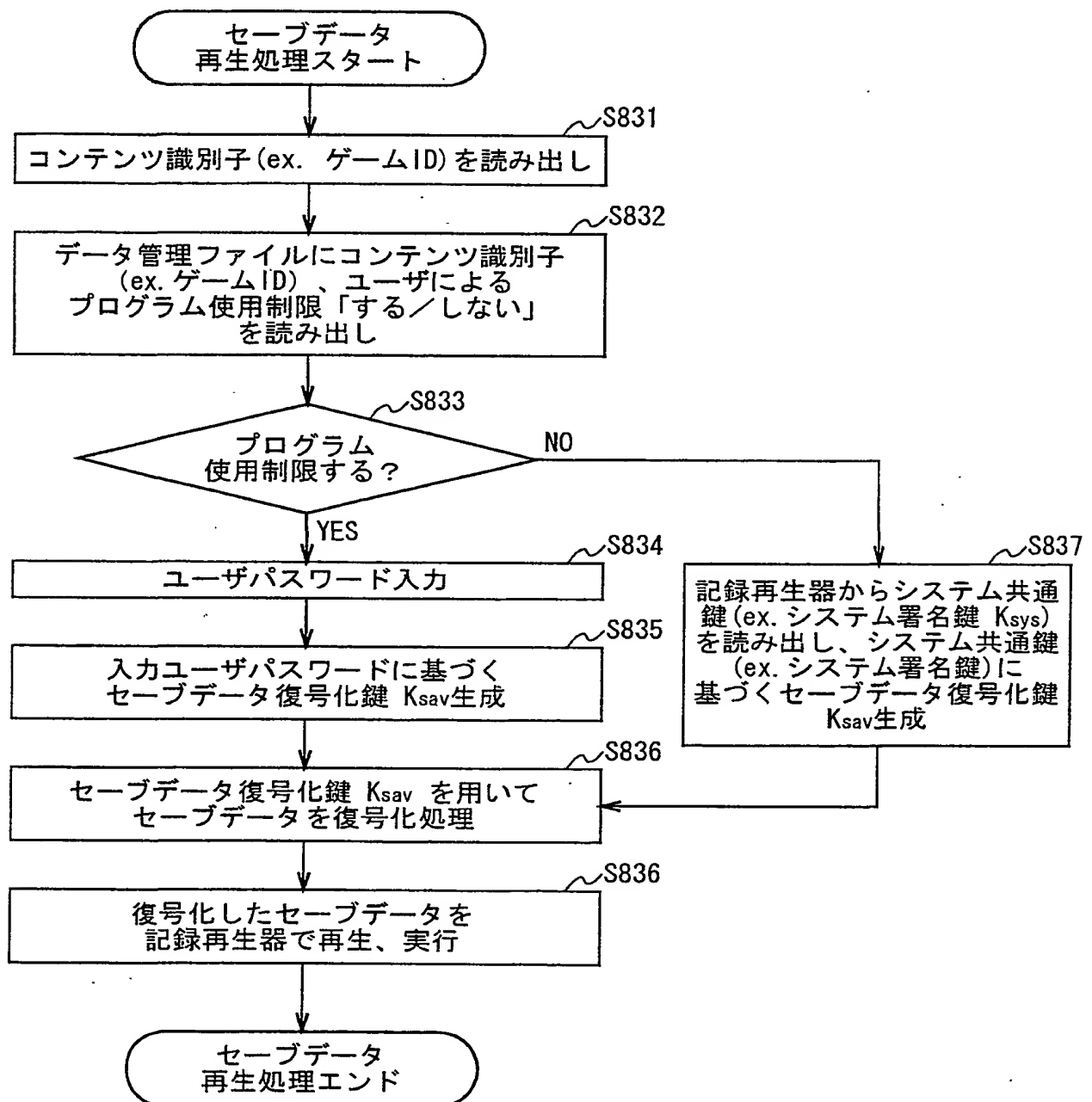
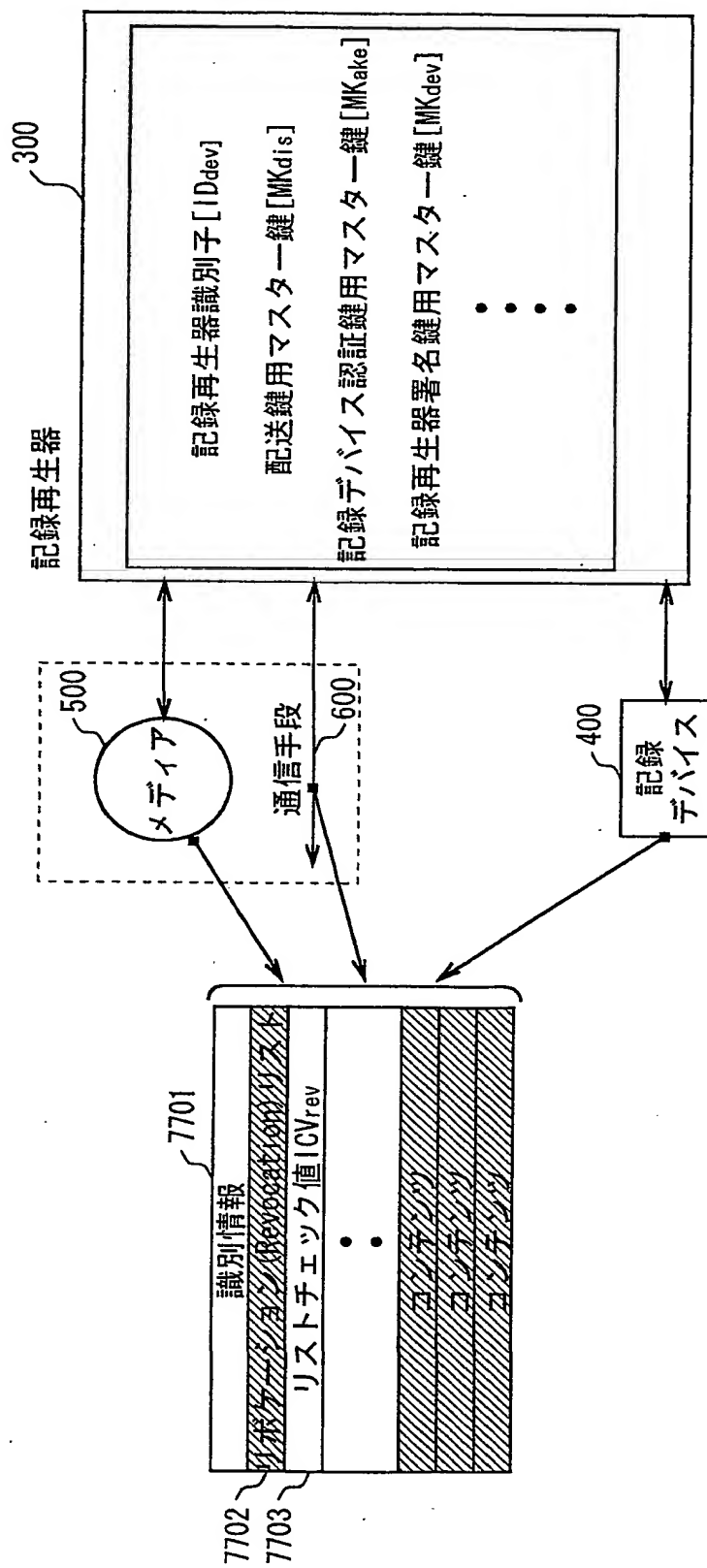


図 8 5



68X

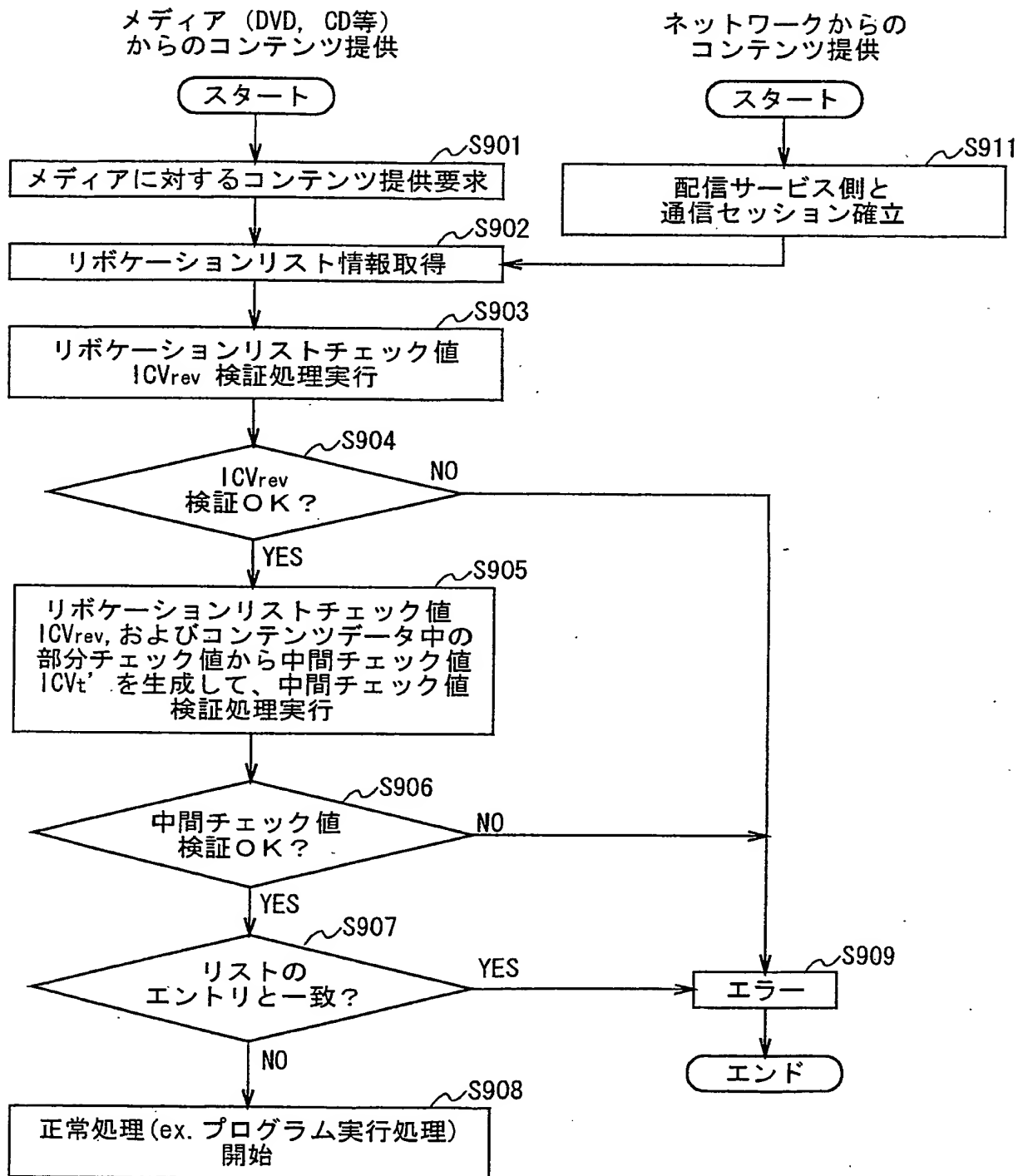


図 8 7

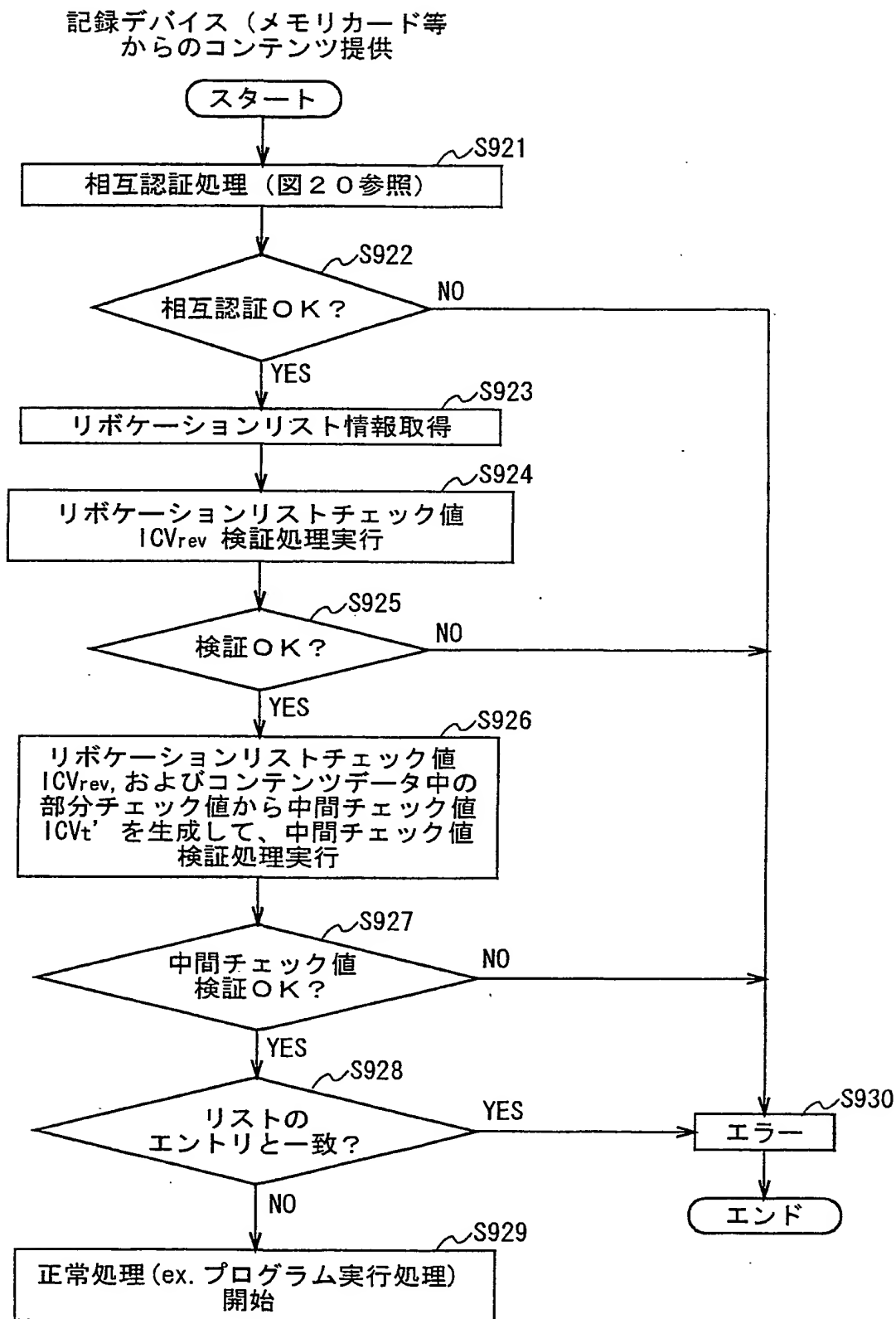


図88

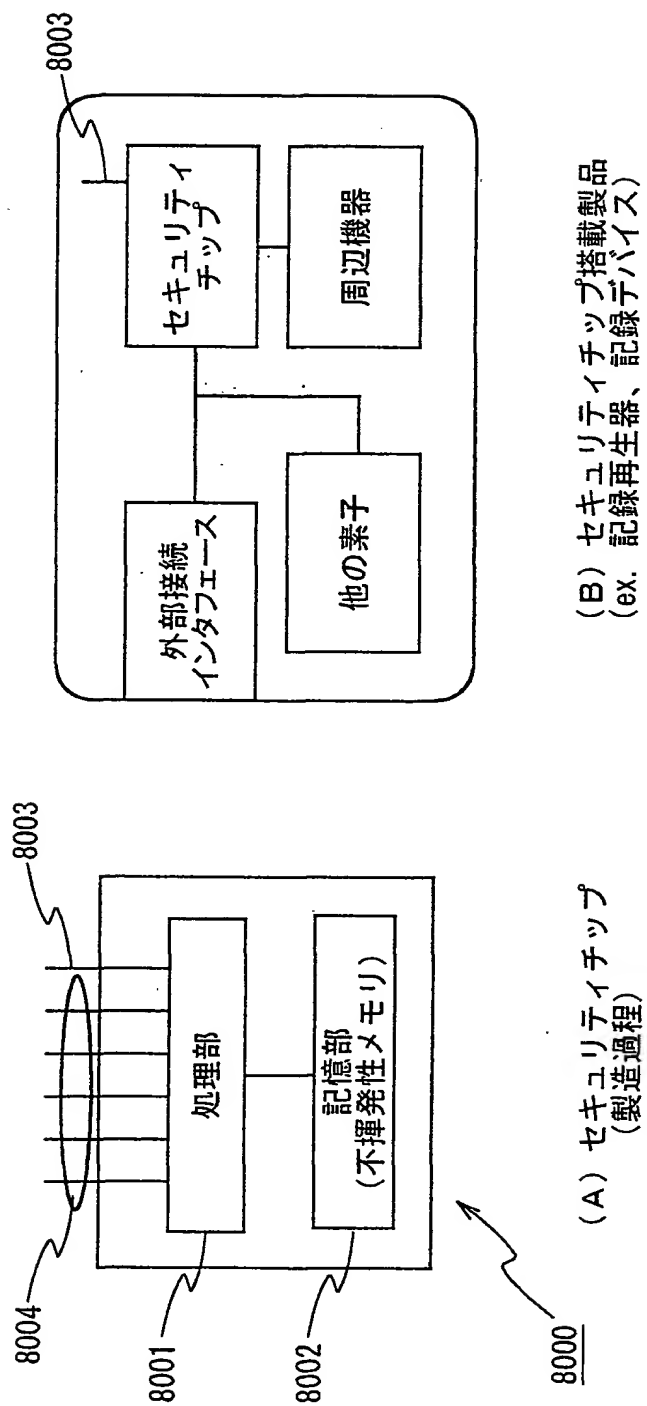


図 89

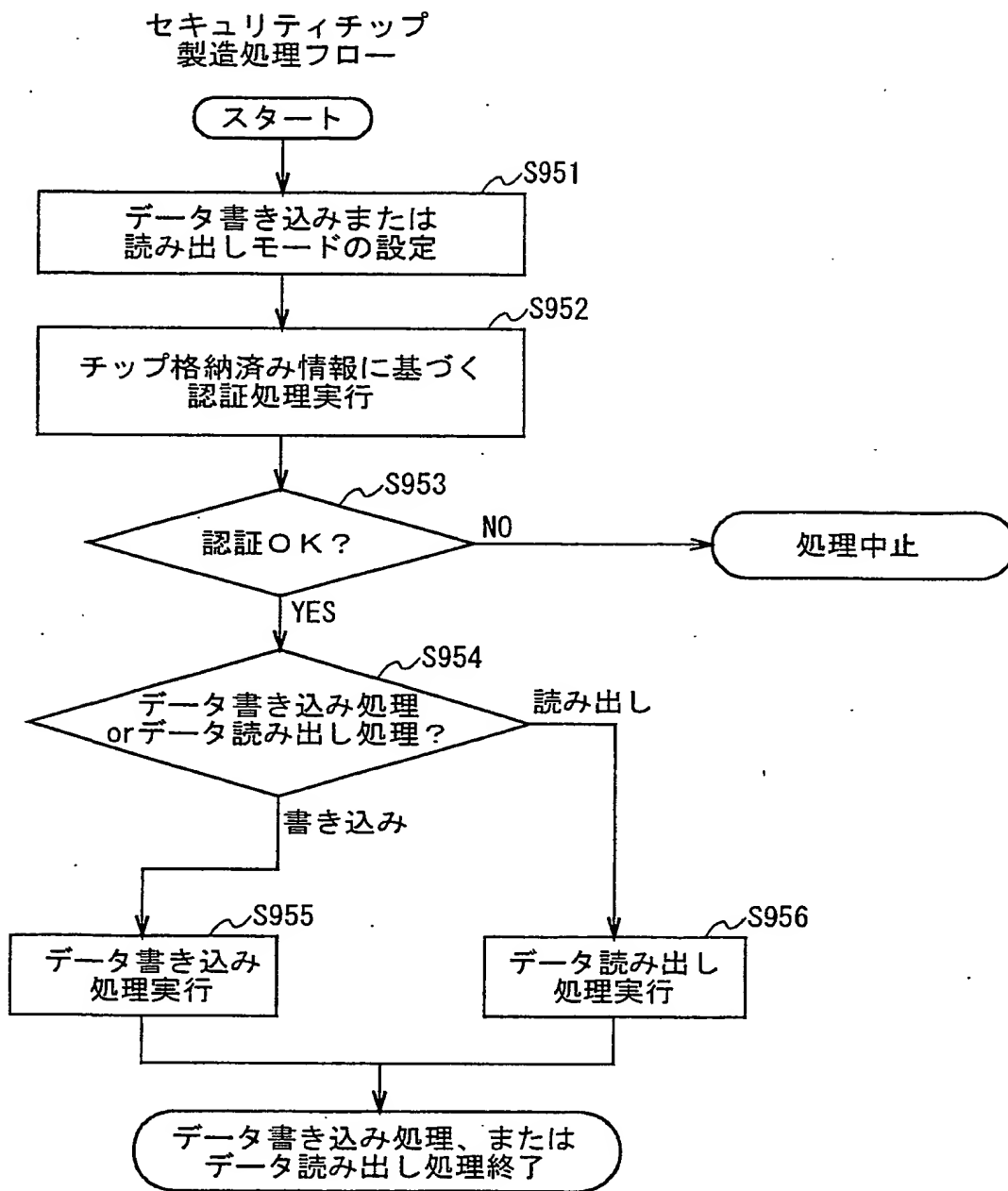


図 9 0

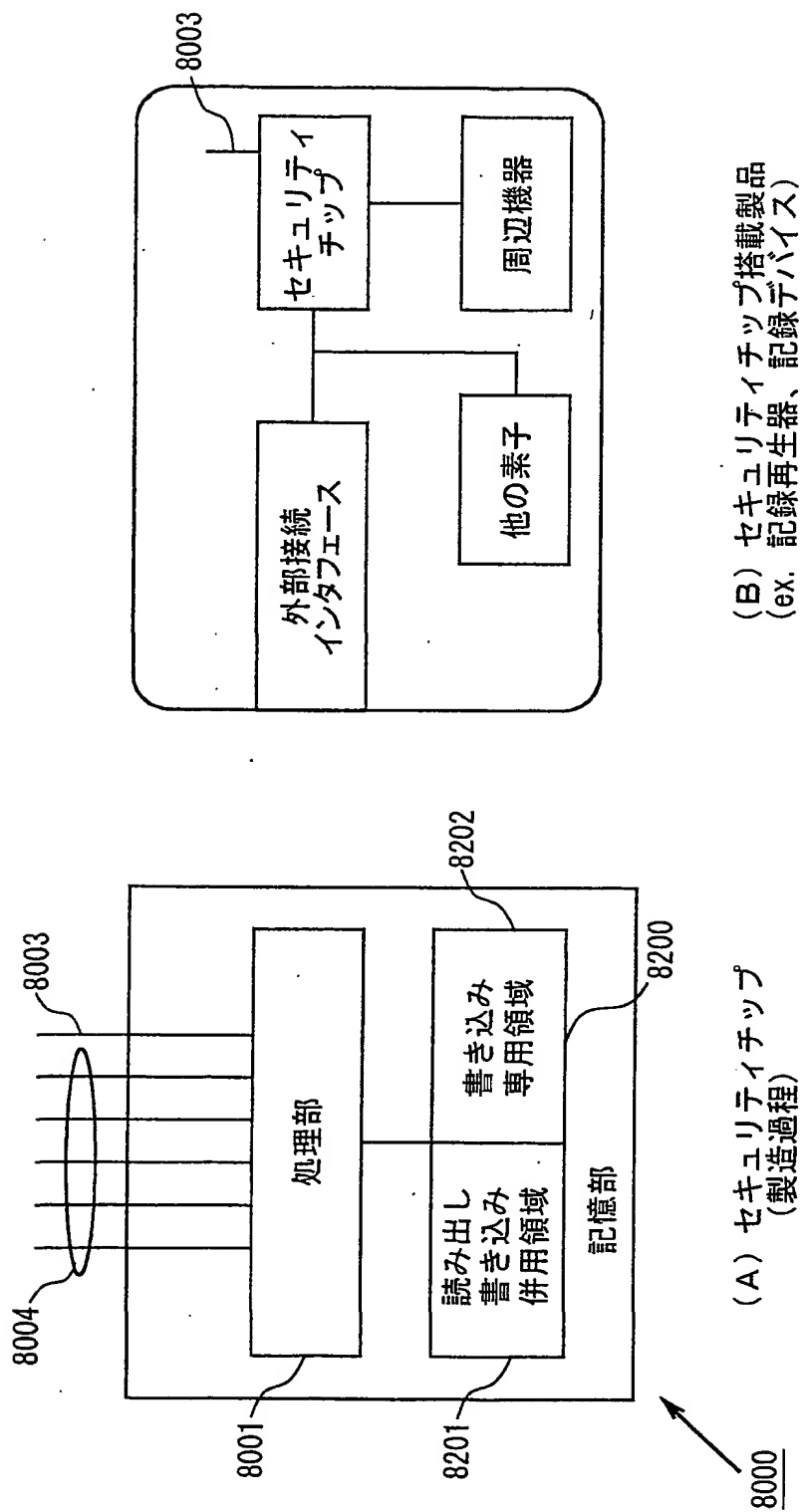


図 9 1

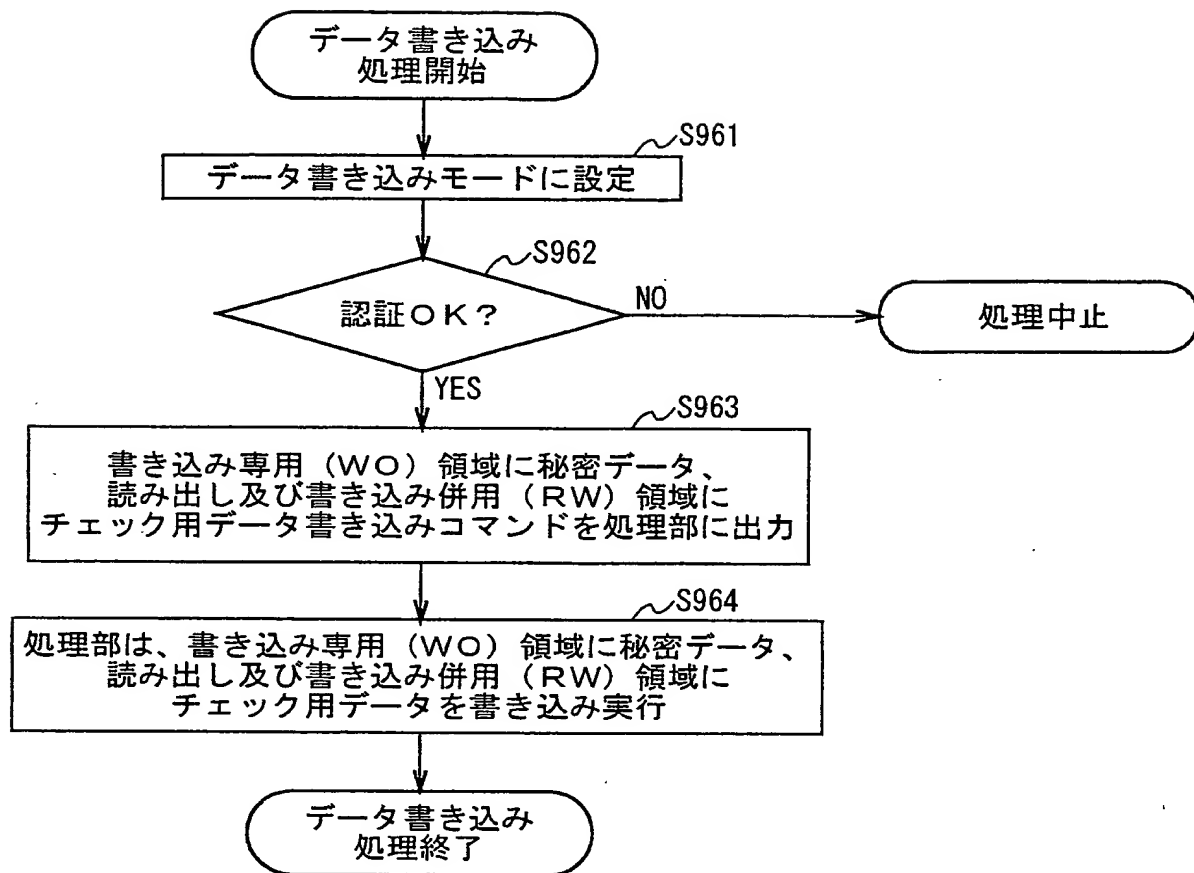


図 9 2

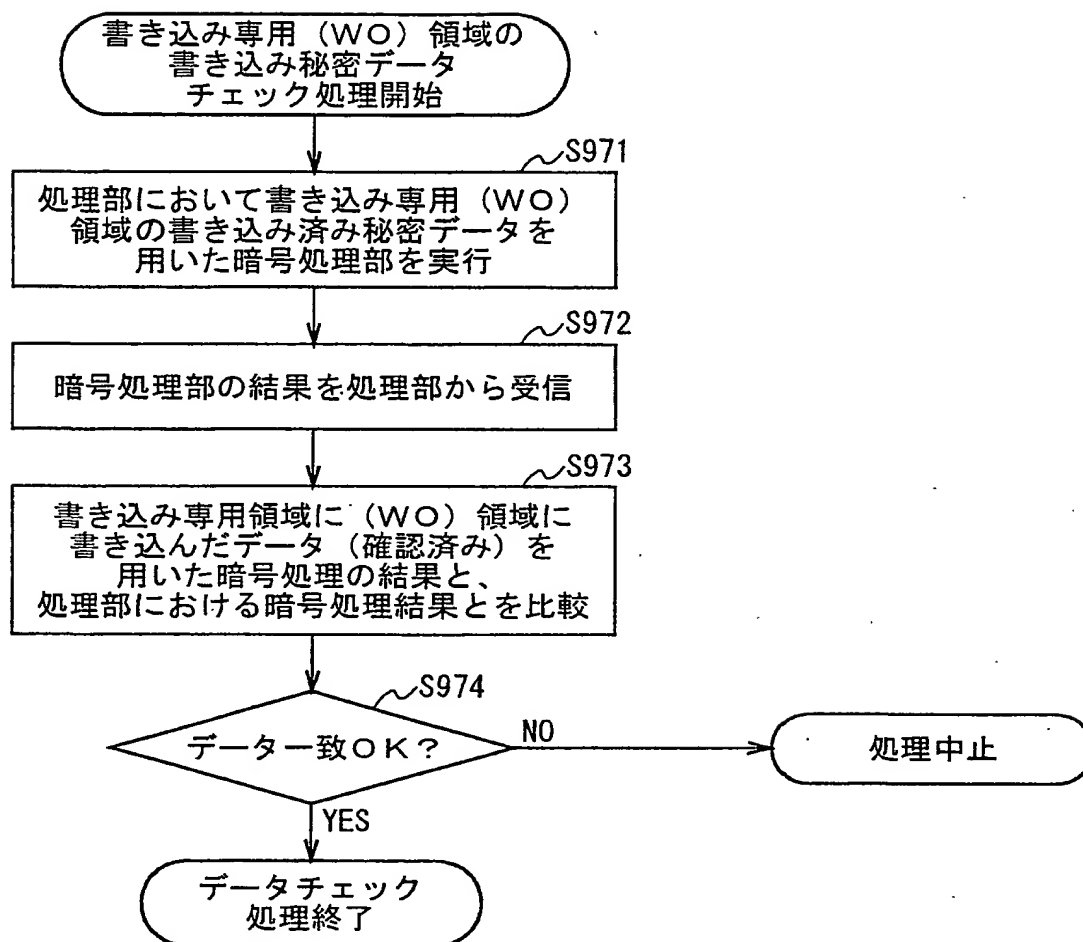


図 9.3

符 号 の 説 明

106...メインCPU、107...RAM、108...ROM、109...AV
処理部、110...入力処理部、111...PIO、112...SIO、300...
記録再生器、301...制御部、302...暗号処理部、303...記録デバイスコ
ントローラ、304...読み取り部、305...通信部、306...制御部、307
...内部メモリ、308...暗号／復号化部、400...記録デバイス、401...
暗号処理部、402...外部メモリ、403...制御部、404...通信部、405
内部メモリ、406...暗号／復号化部、407...外部メモリ制御部、500...
メディア、600...通信手段、2101, 2102, 2103...記録再生器、
2104, 2105, 2106...記録デバイス、2901...コマンド番号管理
部、2902...コマンドレジスタ、2903, 2904...認証フラグ、300
1...スピーカ、3002...モニタ、3090...メモリ、3091...コンテン
ツ解析部、3092...データ記憶部、3093...プログラム記憶部、3094
...圧縮伸長処理部、7701...コンテンツデータ、7702...リボケーション
リスト、7703...リストチェック値、8000...セキュリティチップ、80
01...処理部、8002...記憶部、8003...モード信号線、8004...コ
マンド信号線、8201...読み出し書き込み併用領域、8202...書き込み専
用領域